Compliance Guardian Online 1

User Guide

Service Pack 2, Cumulative Update 2

Issued September 2015

Table of Contents

What's New in this Guide 7

About Compliance Guardian Online 8

Submitting Documentation Feedback to AvePoint 9

Register an Account 10

Resetting your Compliance Guardian Online Password 12

Integration with AvePoint Online Services 13

AvePoint Online Services Versions: Commercial and U.S. Government Public Sector 14

Navigating Compliance Guardian Online 15

Settings 17

System Settings 17

Preference 17

License Manager 18

Auditor 20

Compliance Guardian Online Auditor 20

Auditor Settings 20

Account Manager 21

Group Management 21

User Management 24

Application Profiles 26

Spider Profile 26

Test Suite Manager 31

Check Manager 33

Filter Policy 34

Action Policy 38

User Agent Profile 43

Authentication Profile 44

User Notification Profile 46

Alert Profile 47
Security Profile 49
E-mail Template 49
Compliance Scanner 52
Getting Started 52
Launching Compliance Scanner 52
Managing Scans 52
Creating Scans 53
Creating Scans to Scan Website 53
Creating Scans to Scan SharePoint Online Sites 54
Editing Scans 55
Compliance Reports 56
Launching Compliance Reports 56
Getting Started 56
Compliance Report Home Page 57
Scan Result Overview 58
Risk Report Overview 59
Violation Report Overview 60
Other Reports Overview 60
Types of Compliance Reports 62
Scan Result Report 63
Risk Report 67
Data Table Report 69
File Errors Report 70
File Type Report 71
PDF Exception Report 72
Violation Report 73
Link Validation Report 74
Page Title Report 76
Export Requests 77
Human Auditor 78

Export All Requests to HTML 79
Classification Scanner 84
Getting Started 84
Launching Classification Scanner 84
Managing Scans 84
Creating Scans 85
Selecting Authentication Profile 85
Defining the SharePoint Online Site Scope 85
Configuring Scan Settings 86
Editing Scans 86
Classification Reports 87
Launching Classification Reports 87
Action Report 87
Selecting Scope to Generate Action Report 87
Viewing Action Reports 88
Configuring Settings for Action Report 90
Incident Manager 90
Managing Quarantined Files 91
Managing Encrypted Files 95
Managing Redacted Files 99
Export Requests 103
Job Monitor 104
Getting Started 104
Launching Job Monitor 104
Managing Jobs 104
Appendix A: Accessing Hot Key Mode 105
Compliance Scanner Page 105
Compliance Reports 106
Scan Result 106
Human Auditor 106
Export Requests 106

Export All Requests to HTML 107
Classification Scanner Page 107
Classification Reports 107
Export Requests 108
Preference 108
License Manager 108
Compliance Guardian Online Auditor 108
Auditor Settings 109
Group Management 109
User Management 109
Spider Profile 110
Test Suite Manager 110
Check Manager 110
Filter Policy 111
Action Policy 111
User Agent Profile 112
Authentication Profile 112
User Notification Profile 112
Alert Profile 113
Security Profile 113
E-mail Template 114
Job Monitor 114
Appendix B: Using Transaction Capture 115
Getting Started to Use the Tool 115
Signing in the Tool 116
Using the Tool 116
Hot Key Mode 118
Appendix C: Test Suites and Checks 119
Checks 119
Types of Checks 119
Test Suites 156

Test Suite for Compliance Reporting 157
Test Suite for Classification and Tagging 162
Test Suite for Redaction 166
Appendix D: Supported File Types 168
Notices and Copyright Information 169

What's New in this Guide

- Added information about the U.S. Government Public Sector version of Compliance Guardian Online. Refer to AvePoint Online Services Versions: Commercial and U.S. Government Public Sector.
- Added information about Data Centers when you Register an Account.

About Compliance Guardian Online

Compliance Guardian Online is an online version of Compliance Guardian used to scan websites or SharePoint Online sites for accessibility, privacy, site quality, and security.

Compliance Guardian is designed to ensure that information is available and accessible to the people who should have it and protected from the people who should not. Compliance Guardian helps Chief Privacy Officers, Chief Information Security Officers, Compliance Managers, Records Managers, SharePoint Administrators, and Company Executives proactively protect their IT environments from harmful information leaks, contamination, or misuse while simultaneously ensuring that all activities and content residing in their environments are compliant, accessible, and manageable.

Compliance Guardian is designed to empower organizations to comply with regulatory, statutory, or organization specific requirements to manage and oversee access to sensitive data.

Compliance Guardian works with AvePoint's extended Compliance Solutions to provide a "heat map" that provides additional actionable context about the document including: how old is the document, who authored it, how many times has it been accessed, who can access it, who has accessed it, and what have they done with it. In this way, organizations can take specific steps to protect and mitigate their risk.

By identifying, classifying, and taking action on compliance risks, and presenting this information in easily digestible formats for various stakeholders, organizations can more effectively build and maintain a compliant framework.

Compliance Guardian Online supports the responsive Web design for working on tablet, smart phone, etc.

***Note**: To use Compliance Guardian Online, you must enable cookies and JavaScript.

Access https://www.complianceguardianonline.com to use the version for Commercial use.

Access https://usgov.complianceguardianonline.com to use the U.S. Government Pubic Sector version of Compliance Guardian Online.

Submitting Documentation Feedback to AvePoint

AvePoint encourages customers to provide feedback regarding our product documentation. You can Submit Your Feedback on our website.

Register an Account

Before using the unified Compliance Guardian Online login page URL for all users, each Compliance Guardian Online verifies the user's credentials by itself.

To register a new account, select **Create an account?** You will be brought to the Compliance Guardian Online Register Account page. You will have 14 free days to use Compliance Guardian Online after you register.

***Note**: If you have a trial license, you can only have 10 scans in total, and 100 jobs in total. For more information on a Compliance scan and Classification scan, refer to Compliance Scanner and Classification Scanner.

To register an account, complete the following steps:

1. In the **Register Information** page, configure the following settings:
    - **E-mail Address** – Specify the e-mail address you want to use to login to Compliance Guardian Online.
    - **Data Center** – Select a data center from the drop-down list to create your account. You can select **US - East**, **EMEA - Ireland**, or **APAC - Singapore** from the drop-down list.

      If you use the version available on Microsoft's Cloud Platform for U.S. Government, select the **US Gov Virginia** data center.
    - **First Name** – Enter your first name.
    - **Last Name** – Enter your last name.
    - **Password** – Enter your password to login Compliance Guardian Online.
    - **Confirm Password** – Re-enter your password which is used to login to Compliance Guardian Online.
    - **Country or Region** – Select your country or region. When selecting United States or Canada, you also need to select your state or province.
    - **States or Province** – Select your state or province.
    - **Country Code** – Select your country code.
    - **Phone Number** – Enter your phone number.
    - **Organization Name** – Specify the organization you belong to.
    - **Address** – Enter your address.
    - **City –** Enter the name of the city where you work in the provided text box.
    - **Zip Code –** Enter your zip code in the provided text box.

    Select the **I agree to the Terms of Service** and **Privacy Policy** checkbox and then select **Next**.

2. In the **Scan Source and Message** page, select the scan source:

    - **SharePoint Online Site** – Select the checkbox for scanning SharePoint Online sites. Then, enter the number of user seats for SharePoint Online.
    - **Website** – Select the checkbox for scanning websites. Then, enter the domains you want to scan, specifying three domains at most. Use a semicolon to separate each domain. You can only scan a maximum of three domains during the free trial period of 14 days.

    Add any **Additional Comment** as necessary.

3. Select **Submit** or select **Back** to edit any fields on the **Register Information** page.
4. On the **Confirmation** page, review the registered information, and select **OK**.

Resetting your Compliance Guardian Online Password

If you forget your Compliance Guardian Online password and want to reset a new password, complete the following steps:

1. Navigate to the Compliance Guardian Online **Sign In** page.
2. Select the **Forgot your password?** link under **Sign In** to enter the **Forgot Password** page.
3. Enter the following information on the page:
    - **Login ID** – Enter the e-mail address you used to register with Compliance Guardian Online.
    - **Verification** – Enter the verification characters. Select **Refresh** to refresh the verification graphic if no image is displayed.
4. Select **Submit** to set a new password. After submitting, a verification e-mail is sent to the e-mail you specified.
5. Retrieve the e-mail message and select the supplied link to set a new password. After selecting the link, you will be redirected to the **Forgot Password** page.
6. Enter the following information on the **Forgot Password** page:
    - **New password** – Enter a new password that you want to use.
    - **Confirm password** – Enter the new password again for confirmation.
    - **Verification** – Enter the verification characters. Select **Refresh** to refresh the verification graphic if there is no display image.
7. After setting up the new password, select **Submit** to save your new password. The sign in page appears.
8. Enter your new password to log into Compliance Guardian Online.

Integration with AvePoint Online Services

Compliance Guardian Online is integrated with AvePoint Online Services. Users can register accounts for Compliance Guardian Online in AvePoint Online Services instead of registering it through the unified Compliance Guardian Online login page URL. Access to Compliance Guardian Online is also available through the AvePoint Online Services sign in page. To register for a Compliance Guardian Online account in AvePoint Online Services, you must first register an account in AvePoint Online Services. AvePoint provides the following methods to register an AvePoint Online Services account:

- Register on the AvePoint Online Services website.
- Visit the AvePoint Online Services page or the Compliance Guardian Online page on the AvePoint official website.
- To register for AvePoint Online Services for U.S. Government Public Sector, access the following URL: https://usgov.avepointonlineservices.com.

To access Compliance Guardian Online through AvePoint Online Services, use one of the entries above to sign into AvePoint Online Services. For details, refer to the AvePoint Online Services User Guide.

If you access Compliance Guardian Online through AvePoint Online Service, you are allowed to navigate back to the home page of AvePoint Online Services, or go to other online products. Select the switch product ( ) button on the top of Compliance Guardian Online interface and then select the other online product name to go to the other online product on the navigation bar.

Refer to the following rules for the user permissions in Compliance Guardian Online and AvePoint Online Services.

- Once a user registers a new account through Compliance Guardian Online, the account is synchronized into AvePoint Online Services as the Service Administrator.
- Once a user is added into Compliance Guardian Online power user group, the user will be the Application Administrator of the AvePoint Online Services product.
- Once a user is added into Compliance Guardian Online standard user group, this user is the Standard User in AvePoint Online Services.
- Once a user is deleted from Compliance Guardian Online:
    - If the user is only in Compliance Guardian Online, this user will be totally deleted from AvePoint Online Services.
    - If the user is also in other online products that are integrated in AvePoint Online Services, the user permission will be updated since it is deleted from Compliance Guardian Online, but the user will keep the permission for other online products.
- Once a user's permission is changed in Compliance Guardian Online, the modification will be synchronized into AvePoint Online Services according to the above first three rules.

Refer to the AvePoint Online Services User Guide for detailed information in AvePoint Online Services. Refer to the Account Manager section in this user guide for detailed information on the user permissions in Compliance Guardian Online.

AvePoint Online Services Versions: Commercial and U.S. Government Public Sector

There are two versions of AvePoint Online Services: a version for Commercial use, and a version available on Microsoft's Cloud Platform for U.S. Government. The U.S. Government Public Sector version of AvePoint Online Services offers most of the same functionality as the Commercial version. For details, refer to the AvePoint Online Services User Guide. Functionality of Compliance Guardian Online in both versions is the same.

Navigating Compliance Guardian Online

Compliance Guardian Online shares similar navigation and features that are found in Compliance Guardian on premise.

Here is a sample window in Compliance Guardian Online. It features a familiar, dynamic ribbon, and a searchable, content list view.

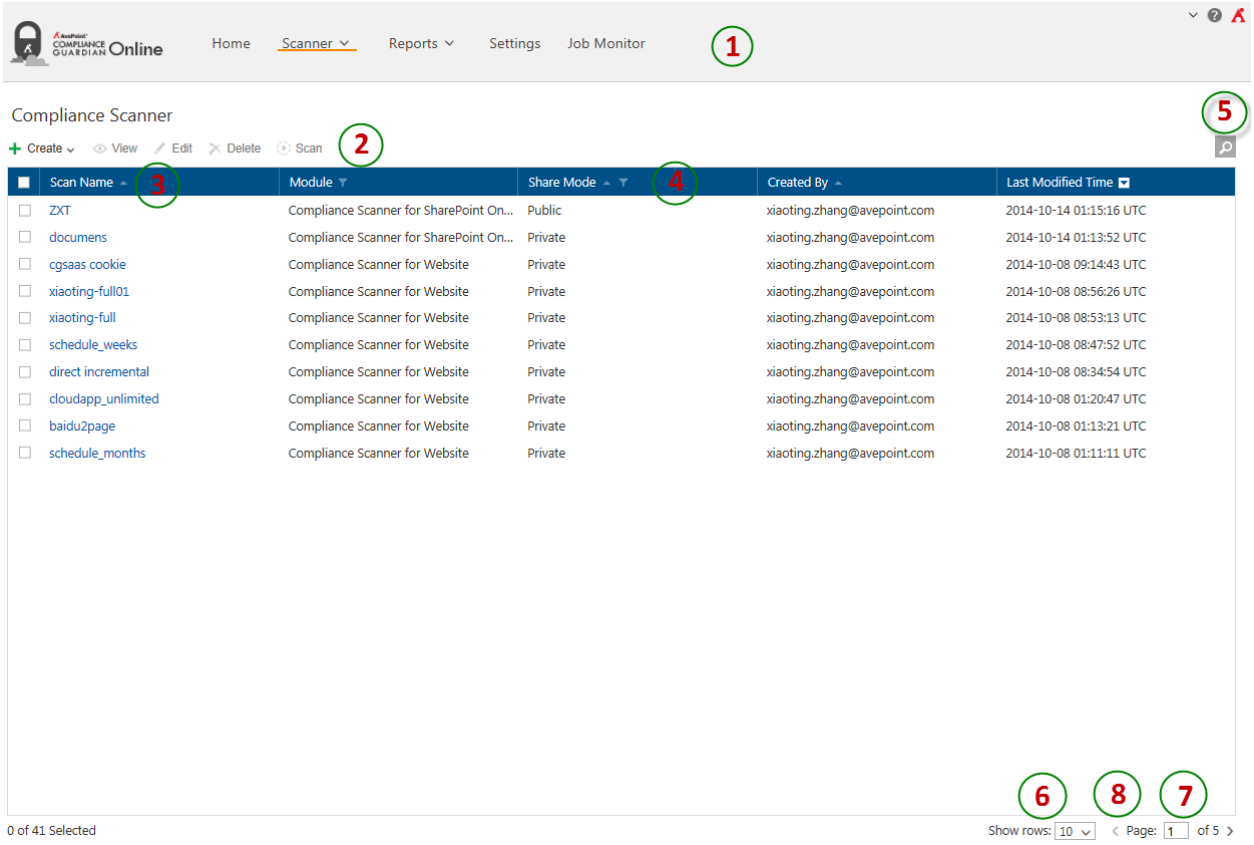

Figure 1: Sample window in Compliance Guardian Online.

1. **Module Pane** – Allows users to quickly navigate between Compliance Guardian Online modules.
2. **Action Field** – Allows users to perform actions to the selected item.
3. **Sort** ( ) – Sort all of the values in the selected column according to the ascending/descending order.
4. **Filter the column** ( ) – Filter the column. Unlike Search, you can filter whichever item you want, rather than search based on a keyword. Hover over the column, and then select the filter the column button ( ), then check the checkbox next to the item name to have that item shown in the list.
5. **Search** – Filter the items and display them by the keyword you designate. At the top-right corner of the viewing pane, enter the keyword for the items you want to display in the text box that appears after selecting the search button ( ).

6. To change the number of items displayed per page, select the desired number from **10** (default value), **15**, **20**, **30** in the **Show rows** drop-down menu at the lower right corner.
7. To go to the specified page, enter the page number in the **Page … of** text box at the lower right corner and press **Enter**.
8. To go to the next page, select the **>** button at the lower right corner. To return to the previous page, select the **<** button at the lower right corner.

Settings

The Settings page is where you customize configurations that affect Compliance Guardian Online as a whole and configure settings that may be only relevant to certain features.

Log into Compliance Guardian Online. Select **Settings** to launch its interface. If you are already in the software, select **Settings** on the top of the interface.

System Settings

System Settings include the Preference settings and License settings.

Preference

Preference allows you to customize Compliance Guardian Online interface itself. To configure the Preference settings, select **Preference** under the **System Settings** heading.

Configure the **Personal Settings** on the **Preference** interface:

- **Specify Your Home Page** – Select the page that will be the home page the next time you log in to Compliance Guardian Online.
- **Time Zone** – Select the time zone for Compliance Guardian Online.

Configure the **Tenant Settings** on the **Preference** interface:

***Note**: Only the power user can view and configure the tenant settings.

- **Page Theme** – Select the page theme.
- **Logo Settings** – Define the logo image used in PC or mobile device. Then enter the alt text for the logo image. Select **Browse**, and then select a header image. Enter the alt text for the header message. Select **Reset** to return to use the default image.
- **Header Settings** – Define the header image. Select **Browse**, and then select a header image. Enter the alt text for the header message. Select **Reset** to return to use the default image.
- **Footer Settings** – Define the footer image. Select **Browse**, and then select a footer image. Enter the alt text for the footer message. Select **Reset** to return to use the default image.

***Note**: You can only upload a .jpg, .jpeg, .jpe, .jfif, .png, .bmp or .dib file as the logo, header or footer image. The image size cannot greater than 5 MB. Select **Apply** to save and apply your settings, or select **Reset** to erase any settings.

License Manager

License Manager provides you with information regarding your Compliance Guardian Online license. To access the interface, select **License Manager** under the **System Settings** heading. You will be brought to the **License Manager** interface that includes the following license information.

The **SharePoint Online** tab displays the license information for scanning SharePoint Online sites:

- **License Information** – The current license information.
  - **License Type** – Whether you have a trial license or an enterprise license.
  - **Number of User Seats** – The number of user seats for SharePoint Online.
  - **Expiration Time** – The expiration time of the license for Compliance Guardian Online.
  - **Status** – The current status of Compliance Guardian Online which reflects proper licensing.
- **Alert Settings** – Compliance Guardian Online can be configured to notify you before licenses expires. You can set how many days prior to expiration and at what interval you want to be notified, as well as configure the method of notification to use.

  To configure the alert settings, select **Alert Settings** and edit as necessary:

  - **Notification Schedule** – Configure the license expiration notification settings. Enter a positive integer into the text box and select **Days** or **Months** from the **Remind me starting __ before my license expires for any module** drop-down menu. Select the **Interval** checkbox to have the reminder repeat at a set interval. Enter a positive integer into the text box and select **Days** or **Months** from the drop-down menu.
  - **Notification Method** – Select the notification method. Select **Pop-up message when you log in** to receive an alert when you log into Compliance Guardian Online. Select **E-mail Notification** to receive an alert by e-mail.

  Select **Apply** to apply the alert settings, or select **Reset** to clear your changes and return to the default settings.

The **Website** tab displays the license information for scanning websites:

- **License Information** – The current license related information.
  - **License Type** – Whether you have a trial license or an enterprise license.
  - **Expiration Time** – The expiration time of the license for Compliance Guardian Online.
  - **Status** – The current status of Compliance Guardian Online which reflects proper licensing.

- **License Details** – The current license details.
    - **Available Domains** – The domains that you can scan.
- **Alert Settings** – Compliance Guardian Online can be configured to notify you before licenses expires. You can set how many days prior to expiration and at what interval you want to be notified, as well as configure the method of notification to use.

  To configure the alert settings, select **Alert Settings** and edit as necessary:

    - **Notification Schedule** – Configure the license expiration notification settings. Enter a positive integer into the text box and select **Days** or **Months** from the **Remind me starting __ before my license expires for any module** drop-down menu. Select the **Interval** checkbox to have the reminder repeat at a set interval. Enter a positive integer into the text box and select **Days** or **Months** from the drop-down menu.
    - **Notification Method** – Select the notification method. Select **Pop-up message when you log in** to receive an alert when you log into Compliance Guardian Online. Select **E-mail Notification** to receive an alert by e-mail.

  Select **Apply** to apply the alert settings, or select **Reset** to clear your changes and return to the default settings.

You can extend your license by selecting **Extend License** above the License Information section of the License Manager interface.

To extend a SharePoint Online license, configure the following settings on the **SharePoint Online** tab:

- **User ID** – Displays your login ID.
- **License Type** – Displays your license type.
- **Extend Duration** – Specify the time that you want to extend your use of Compliance Guardian Online.
- **Number of User Seats** – Specify the required number of user seats.
- **Comment** – Enter any comment to explain why you want to extend your license.

***Note**: The users in the Standard User Group cannot extend a license. For more information on the Standard User Group, refer to Power Administrator Group and Standard User Group.

To extend a website license, configure the following settings on the **Website** tab:

- **User ID** – Displays your login ID.
- **License Type** – Displays your license type.
- **Extend Duration** – Specify the time that you want to extend your use of website.
- **Domains** – Enter the domains where the webpages you want to scan reside. The domains that you have purchased are also displayed here.

- **Comment** – Enter any comment to explain why you want to extend your license.

Select **Reset** to reset the settings in the **Extend License** interface, or select **Submit** to submit the application to your AvePoint representative for extending your license.

If your license has been extended to be an enterprise license, the next time you log into Compliance Guardian Online, the **License Agreement** interface appears. You must accept the Compliance Guardian Online license agreement before you can continue to use Compliance Guardian Online.

Auditor

Auditor monitors the activities in Compliance Guardian Online, such as creating, modifying, or deleting a scan, exporting a report, or making changes on test suite, etc. It also allows you to view and export the desired auditor data report.

Compliance Guardian Online Auditor

To access **Compliance Guardian Online Auditor** in the **Settings** interface, select **Compliance Guardian Online Auditor** under the **Auditor** heading.

In the Compliance Guardian Online Auditor interface, you will see all of the activities and the related information including the users of the activities, the groups to which the users belong, the time of the activities, the modules in which the activities are performed, and the statuses of the activities.

***Note**: The users in the Standard User Group can only view their own activities in Compliance Guardian Online, while the users in the Power Administrator Group can view all of the other users' activities. For more information on the Power Administrator Group and Standard User Group, refer to Power Administrator Group and Standard User Group.

You can search the information displayed by designating the keyword. The keyword must be contained in the **User**, **Group**, **Module**, **Object** or **Event** column value. Above the auditor data viewing pane, select on the search ( ) button, and the **Enter keyword** text box appears. Then, enter the keyword and select the search ( ) button to search for the information you want to display.

Exporting Auditor Data Report

The auditor data displayed in Compliance Guardian Online Auditor can be easily exported to a datasheet for further review. Select **Export to Datasheet** on the upper-right corner of the **Compliance Guardian Online Auditor** interface, save the report to your desired location, and then review it in the datasheet.

Auditor Settings

If you want to view and store all the activities that users perform in Compliance Guardian Online, configure the auditor settings to your desired auditor data in the Compliance Guardian Online Auditor.

To access **Auditor Settings** in the **Settings** interface, select **Auditor Settings** under the **Auditor** heading.

***Note**: The users in the Standard User Group cannot configure settings in Auditor Settings. For more information on the Standard User Group, refer to Power Administrator Group and Standard User Group.

In the **Auditor Settings** interface, configure the following settings:

- **Pruning Rule** – Enter a value in the **Keep the data in the last _ Days/Weeks/Months** field. The activities audited within the specified time range will be displayed in the **Compliance Guardian Online Auditor** interface.
- **Audited Actions** – Select the action types that will be displayed in the **Compliance Guardian Online Auditor** interface. By default, the **Create** type action, **Update** type action, and **Delete** type action are selected.

Select **Apply** to apply the settings. Select **Reset** to erase the current settings and display the previously applied settings.

***Note:** You can only use the **Reset** button for settings that have not yet been applied.

After you select **Apply**, the **Pruning Rule** setting will be applied at 9 am UTC. The activities audited within the specified time range in the **Pruning Rule** field will be displayed in the **Compliance Guardian Online Auditor** interface from 9 am UTC. Related information about the actions performed before you applied the auditor settings will not be changed (in the **Compliance Guardian Online Auditor** interface) according to the action types you selected in the **Audit Action** field. However, related information about the actions performed after you applied the auditor settings will be displayed according to the action type you selected in the **Audit Action** field.

Account Manager

Account Manager allows you to view and manage users and configure user groups with custom permissions for Compliance Guardian Online. This module allows you to give specific people, or groups of people your desired level of access to Compliance Guardian Online.

In Account Manager you can give specified permissions to Compliance Guardian Online users to limit which Compliance Guardian Online module a user is able to access. A user can belong to multiple groups.

Group Management

Group Management allows you to manage groups. To access **Group Management** for Compliance Guardian Online in the **Settings** interface, select **Group Management** under the Account Manager heading.

Power Administrator Group and Standard User Group

The Power Administrator Group users have Full Control permissions to use Compliance Guardian Online. It cannot be deleted or removed from the Power Administrator Group. The registered user can add users to the group.

The Standard User Group is another group in Compliance Guardian Online. It also cannot be deleted. The registered user must first edit this group to assign permissions to the group, and add users to this group.

***Note**: The users in the Standard User Group cannot extend a license, use **Account Manager**, use **Auditor Settings**, use **Test Suite Manager**, or use **Check Manager** in Compliance Guardian Online although the group has the **Settings** permission.

Managing Groups

In the **Group Management** interface, you will see a list of previously configured groups.

Creating and Editing Groups

To create a new group, select **Create** in the **Group Management** page. To modify a previously configured group, select the group, and then select **Edit**. In the Create Group or Edit Group interface, configure the following settings:

- **Group Name** – Enter a group name.
- **Permissions** – Select the permissions for the group.
    - **Compliance** – Compliance includes **Compliance Scanner** and **Compliance Reports**. If you select the Compliance checkbox, all of the checkboxes before Compliance Scanner and Compliance Reports will be selected.
        - **Compliance Scanner** – Select the **Compliance Scanner** checkbox to give the group users access to use Compliance Scanner in Compliance Guardian Online.
        - **Compliance Reports** – Select the **Compliance Reports** checkbox to give the group users access to use Compliance Reports in Compliance Guardian Online.
            - **Report Sources** – Select the **Report Sources** checkbox, the group users can view all of the scan reports on website and SharePoint Online sites in the Compliance Reports. Select the expand () button, then you can select to just give the group users permission to view the reports on website or reports on SharePoint Online sites.
            - **Report Details** – Select the **Report Details** checkbox, the group users will have the permission to view job details. Select the

expand (⊞) button, then you can select to just give the group users permission to view detailed report or view error highlight.

- **Actions** – Select the **Actions** checkbox to give the group users the permission to export report to datasheet and export all requests to HTML. Select the expand (⊞) button, then you can select to just give the group users permission to export report to datasheet or export all requests to HTML.
- **Human Auditor** – Select the **Human Auditor** checkbox to give the group user to use **Compliance Reports** > **Human Auditor**. The group users can also change the file's status in the **Compliance Reports** > **Scan Result** > **View Detailed Report.**

- **Classification** – Classification includes **Classification Scanner** and **Classification Reports**. If you select the Classification checkbox, all of the checkboxes before Classification Scanner and Classification Reports will be selected.
  - **Classification Scanner** – Select the **Classification Scanner** checkbox to give the group users access to use Classification Scanner in Compliance Guardian Online.
  - **Classification Report** – Select the **Classification Reports** checkbox to give the group users access to use Classification Reports in Compliance Guardian Online.
    - **Report Sources** – Select the **Report Sources** checkbox, the group users can view all of the scan reports on SharePoint Online sites in the Classification Reports.
    - **Report Details** – Select the **Report Details** checkbox to give the group users the permission to view report details.
    - **Incident Types** – Select the **Incident Types** checkbox to give the group users the permission to manage files in Incident Manager. Select the expand (⊞) button, then you can select to just give the group users permission to manage the quarantined files, encrypted files or redacted files.
    - **Actions** – Select the **Actions** checkbox to give the group users the permission to perform actions in Incident Manager. Select the expand (⊞) button, then you can select to just give the users the specified action permissions.
- **Common** – Common includes **Settings** and **Create Shared Policies, Profiles and Scans**. If you select the Common checkbox, both of the checkboxes before **Settings** and **Create Shared Policies, Profiles and Scans** will be selected.
  - **Settings** – Select the **Settings** checkbox to give the group users access to use Settings in Compliance Guardian Online.

***Note**: The users in the created group cannot extend a license, cannot use **Account Manager**, **Auditor Settings**, **Test Suite Manager**, and **Check Manager** although you have selected **Settings** for the group.

- **Create Shared Policies, Profiles and Scans** – Select the **Create Shared Policies, Profiles and Scans** checkbox to give the group users access to set their scans and profiles to **Public** as the Share Mode (all users can see the scans or profiles the user created if the Share Mode of the scans or profiles is **Public**).

- **Users in the Group** – Add users to the group or remove users from the group. To add users to the group, select **Add Users**. The Add Users interface appears. All the existing users are listed in the interface. Select the users that you want to add to the group by selecting the checkboxes before the users, and select **Add Users**. The **Create Group or Edit Group** interface appears again, and the previously selected users that you want to add are listed in the table of the **Users in the Group** field. If you want to remove any users, select the users in the table, and select **Remove Users** above the table.

  To go to the specified page of the table, enter the page number in the **Page … of** text box at the lower right corner and press **Enter**. To go to the next page, select the **>** button at the lower right corner. To return to the previous page, select the **<** button at the lower right corner.

Select **Save** to save the changes so all of the users in the table of **Users in the Group** field will be added in the group, or select **Cancel** to return to the **Group Management** interface without any changes.

Viewing Details about a Group

Select a group, or select the checkbox before the group, and select **View** to see the details of the selected group. Here you can also select **Edit** to make changes to the group's settings. You will be brought to the **Edit** page where you can change the settings for this group. After editing the settings, select **Save** to save the changes, select **Cancel** to return to the **Group Management** interface without saving any of your changes.

Deleting Groups

Select **Delete** to delete any selected groups. A warning message will appear to confirm the deletion. Select **OK** to delete the selected groups, or select **Cancel** to return to the **Group Management** interface without deleting the selected groups. If the selected group contains any active users, the group cannot be deleted.

User Management

User Management allows you to manage specific users. To access **User Management** for Compliance Guardian Online in the **Settings** interface, select **User Management** under the Account Manager heading.

Managing Users

In the **User Management** interface, you will see a list of users.

Inviting Users and Re-sending Invitation to Users

To invite a user, complete the following steps:

1. Select **Invite User** to invite a user to use Compliance Guardian Online.
2. In the **Invite User** interface, configure the following settings:
    - **Users** – Enter the e-mail addresses of the users you want to invite. If you are in a free trial version of Compliance Guardian Online, you can invite 10 users in total. If you are using the official version of Compliance Guardian Online, the number of users you can invite is unlimited.
    - **Select Groups** – Select the groups to which the invited users will be added.
    - **Send Message** – Specify the message in the invitation e-mail.
3. Select **Send** to send the invitation e-mail, or select **Cancel** to return to the **User Management** interface without saving any changes.

    The invited user will receive an invitation e-mail.

If you are the invited user, complete the following steps to activate your account:

1. Select the activation URL in the e-mail to activate the account for using Compliance Guardian Online. The **Activate Account** interface appears.
2. Configure the following settings:
    - **First Name** – Enter your first name.
    - **Last Name** – Enter your last name.
    - **Password** – Enter your password used to log into Compliance Guardian Online.
    - **Re-enter Password** – Re-enter your password.
3. Select **Activate** to activate your account. You can now use Compliance Guardian Online.

If an invited users does not activate their account, you can select the user in the User Management interface, and then select **Re-send Invitation** to send the invitation e-mail to the user again.

***Note**: The invited user must use the activation URL to activate the account within 7 days, or the activation URL will expire.

Viewing Details about a User

Select a user, or select the checkbox before the user, and select **View** to see details about the selected user. Here you can also select **Edit** to make changes to the user's settings. You will be brought to the **Edit** page where you can change the settings for this user. After editing the settings, select **Save** to save

the changes, or select **Cancel** to return to the **User Management** interface without saving any of your changes.

Editing Users

Select the user you want to edit, and then select **Edit**. The **Edit User** interface appears. You can edit the following user information in this interface:

- **E-mail Address** – The e-mail address of the user. You cannot edit or change the email address that was used to register the account.
- **First Name** – The first name of the user.
- **Last Name** – The last name of the user.
- **Permissions** – The groups to which the user belongs.
- **Invited Time** – The time that the user was invited to use Compliance Guardian Online. This cannot be edited.
- **Invited By** – The user who invited this user. This cannot be edited.

Deleting Users

Select **Delete** to delete the selected users. A warning message will appear to confirm the deletion. Select **OK** to delete the selected user, or select **Cancel** to return to the **User Management** interface without deleting the selected user.

Adding Users to Group

Select a user, and then select **Add to Group**. The **Add to Group** window appears. Select the **Select Groups** drop-down list, and select the groups to which the user will be added by selecting the checkboxes before the groups. Select **OK** in the **Add to Group** window to save changes or select **Cancel** without saving any changes.

Application Profiles

Application Profiles provide configuration settings for profiles, policies, and suites throughout the Compliance Guardian Online product including the Spider Profile, Test Suite Manager, Check Manager, Filter Policy, Action Policy, User Agent Profile, Authentication Profile, User Notification Profile, Alert Profile, and E-mail Template. For more information, refer to the following sections.

Spider Profile

A spider profile is used to configure the crawl related settings. Select **Spider Profile** under the **Application Profile** heading. You will be brought to the **Spider Profile** interface.

Managing Spider Profile

In the **Spider Profile** interface, you will see a list of previously configured spider profiles.

You may perform any of the following actions on a selected spider profile:

- **Create** – Select **Create** to create a new spider profile. Refer to the Creating or Editing Spider Profiles section for the details.
- **View** – Select **View** to see the details of the selected spider profile. Here you can also select **Edit** to make changes to the spider profile's settings. You will be brought to the **Edit** page where you can change the settings for this spider profile. After editing the settings, select **Save** to save the scan. To save a changed spider profile as a new one, select **Save As**. At any time, select **Cancel** to return to the **Spider Profile** interface without saving any of your changes.
- **Edit** – Select **Edit** to make changes to the selected spider profile's settings. You will be brought to the **Edit** page where you can change the settings for this scan. Select **Save** to save the scan. To save a changed spider profile as a new one, select **Save As**. At any time, select **Cancel** to return to the **Spider Profile** interface without saving any of your changes.
- **Delete** – Select **Delete** to delete the selected spider profiles. A warning message will appear to confirm the deletion. Select **OK** to delete the selected plan, or select **Cancel** to return to **Spider Profile** interface without deleting the selected spider profiles.

Creating or Editing Spider Profiles

Compliance Guardian Online provides three types of spider profiles that are used in Compliance Scanner and Classification Scanner. Refer to the following section for details.

Creating or Editing Spider Profiles for Scanning Websites in Compliance Scanner

To create a new spider profile for scanning websites in Compliance Scanner, complete the following steps:

1. Select **Create** in the **Spider Profile** interface. Then, select **For Website** in the drop-down list. To modify a previously configured spider profile, select the spider profile, and then select **Edit**. The **Create Spider Profile** or **Edit Spider Profile** interface appears.
2. Configure the following settings:
    - **Spider Profile Name** – Enter a spider profile name. Select the checkbox before **Set as Default** to save the spider profile as the default one.
    - **Share Mode** – Select the share mode. If **Public** is selected, all users can see the spider profile you created; if **Private** is selected, only you can see the spider profile.
    - **Maximum Depth** – It's used to specify the depth level needed to crawl. For example, if you enter **1**, Compliance Guardian Online will only crawl the start URL specified in the scan and then scan the objects in the URL. If you enter **3**, Compliance Guardian Online will crawl the start URL specified in the corresponding scan, the linked pages on the start

URL page, and the linked pages from the pages one level deeper. If you have a trial license, you can specify 100 at most; if you have an enterprise license, you can scan all the pages of an entire website. Enter **unlimited** if you want to scan all the pages of an entire website.

- **Filter Policy** – Select a defined filter policy to limit the objects that will be crawled.
- **Robot Exclusion Protocol Control** – Select whether or not to follow Robot Exclusion Protocol. Unless manually configured, the checkbox is selected, which means that Compliance Guardian Online will not crawl any link that is forbidden to access in **Robot.txt**.
- **Redirection Crawling Control** – Select whether or not to **allow crawling redirections**. If you want to allow crawling redirections, specify the **Maximum redirections allowed** for one page. By default, the checkbox is selected, and the default maximum allowed redirections are **10**.
- **Crawl Option** – Select whether or not to crawl the data that are loaded dynamically using JavaScript.
- **User Agent Profile** – Select the saved user agent profile to specify the user agent for the backend Web server when scanning the webpage. A pre-defined user agent profile can be used directly. Select **New User Agent** to create a new user agent profile.
- **Authentication Method** – Select the Authentication Profile used to connect to the webpage.
- **Timeout of One Scan** – Specify the maximum time of one scan. The value is **7 days** unless manually configured
- **Timeout of Link** – Specify the maximum time of waiting for a response from a link before skipping it during a crawl. The value is **100 seconds** unless manually configured
- **Delay One Link** – Specify the interval time between scanning two links. If you have selected the **Enable rendered crawl** option in the **Crawl Option** field, this value is also used as the delayed time to wait for loading data in a webpage.
- **Report Group** – Select a report group from the drop-down list. You can search the specified groups by entering a keyword in the search field in the drop-down list. Once a group is specified as the Report Group, all of the users in the specified group will be able to view and download the reports in the Compliance Report module. Multiple groups can be specified here; choose **Select All** to select all of the listed groups.
- **Schedule** – Configure the scan schedule by selecting the **Enable scan schedule** checkbox.
- **E-mail Notification** – Choose the notification profile for receiving the scan information. Open the drop-down menu, and select a notification profile you previously created or select **New Notification Profile** to create a new one. For information on creating a notification profile, refer to Creating and Editing User Notification Profile for details. Select Refresh to refresh the information in the drop-down menu.

3. Select **Save** to save the configurations and return to the **Spider Profile** interface. If you edit a spider profile, select **Save As** to save the profile to another one. At any time, select **Cancel** to return to the **Spider Profile** interface without saving any changes.

Creating or Editing Spider Profiles for Scanning SharePoint Online Sites in Compliance Scanner

To create a new spider profile for scanning SharePoint Online sites in Compliance Scanner, complete the following steps:

1. Select **Create** in the **Spider Profile** interface.
2. Select **For SharePoint Online** in the drop-down list. To modify a previously configured spider profile, select the spider profile, and then select **Edit**. The Create Spider Profile or Edit Spider Profile interface appears.
3. Configure the following settings:
    - **Spider Profile Name** – Enter a spider profile name. Select the checkbox before **Set as Default** to save the spider profile as the default one.
    - **Share Mode** – Select the share mode. If **Public** is selected, all users can see the spider profile you created; if **Private** is selected, only you can see the spider profile.
    - **Filter Policy** – Specify a defined filter policy to limit the objects that will be crawled.
    - **Content Option** – Specify the contents that will be scanned within the specified scope.
        - **Include user content** – This checkbox is selected by default, and only the files and items that are created by the end users will be scanned in the specified scope.
        - **Include system content** – Select this checkbox to also scan the system built-in contents in the specified scope.
    - **Scan File/Item Versions** – Specify the method of scanning file/item versions:
        - **Scan the current version** – Only the current versions of the files/items defined in the job scope are supported to be scanned.
        - **Scan all versions** – The files/items and all their previous versions defined in the job scope are supported to be scanned. If this option is selected, the scan result of each file/item version will be reported in the Compliance report separately.
    - **Alert Profile** – Select an alert profile that will be sent when a file fails to be scanned, or there is a violation found in the file. Select **New Alert Profile** to create a new alert profile. For more information, refer to Creating and Editing Alert Profiles.
    - **Report Group** – Select a report group from the drop-down list. Once a group is specified as the Report Group, all of the users in the specified group will be able to view and download the reports in the Compliance Report module. Multiple groups can be specified here; choose **Select All** to select all of the listed groups.
    - **Schedule** – Configure the scan schedule by selecting the **Enable scan schedule** checkbox.

- **E-mail Notification** – Choose the notification profile for receiving the scan information. Open the drop-down menu, and select a notification profile you previously created or select **New Notification Profile** to create a new one. For information on creating a notification profile, refer to Creating and Editing User Notification Profile for details. Select Refresh to refresh the information in the drop-down menu.

4. Select **Save** to save the configurations and return to the **Spider Profile** interface. If you edit a spider profile, select **Save As** to save the profile to another one. At any time, select **Cancel** to return to the **Spider Profile** interface without saving any changes.

Creating or Editing Spider Profiles for Scanning SharePoint Online Sites in Classification Scanner

To create a new spider profile for scanning SharePoint Online sites in Classification Scanner, complete the following steps:

1. Select **Create** in the **Spider Profile** interface.
2. Select **For Classification** in the drop-down list. To modify a previously configured spider profile, select the spider profile, and then select **Edit**. The Create Spider Profile or Edit Spider Profile interface appears.
3. Configure the following settings:
    - **Spider Profile Name** – Enter a spider profile name. Select the checkbox before **Set as Default** to save the spider profile as the default one.
    - **Share Mode** – Select the share mode. If **Public** is selected, all users can see the spider profile you created; if **Private** is selected, only you can see the spider profile.
    - **Filter Policy** – Specify a defined filter policy to limit the objects that will be crawled.
    - **Scan File/Item Versions** – Specify the method of scanning file/item versions:
        - **Scan the current version** – Only the current versions of the files/items defined in the job scope are supported to be scanned.
        - **Scan all versions** – The files/items and all their previous versions defined in the job scope are supported to be scanned. If this option is selected, the scan result of each file/item version will be reported in the Compliance report separately.
    - **Alert Profile** – Select an alert profile that will be sent when a file fails to add a tag. Select **New Alert Profile** to create a new alert profile. For more information, refer to Creating and Editing Alert Profiles.
    - **Report Group** – Select a report group from the drop-down list. Once a group is specified as the Report Group, all of the users in the specified group will be able to access Action Report in Classification Reports. Multiple groups can be specified here; choose **Select All** to select all of the listed groups.
    - **Schedule** – Configure the scan schedule by selecting the **Enable scan schedule** checkbox.

- **E-mail Notification** – Choose the notification profile for receiving the job information. Open the drop-down menu, and select a notification profile you previously created or select **New Notification Profile** to create a new one. For information on creating a notification profile, refer to Creating and Editing User Notification Profile for details. Select Refresh to refresh the information in the drop-down menu.

4. Select **Save** to save the configurations and return to the **Spider Profile** interface. If you edit a spider profile, select **Save As** to save the profile. At any time, select **Cancel** to return to the **Spider Profile** interface without saving any changes.

Test Suite Manager

Test Suite Manager allows you to manage test suites. To access **Test Suite Manager** settings in the **Settings** interface, select **Test Suite Manager** under the **Application Profiles** heading.

Managing Test Suites

In the **Test Suite Manager** interface, you will see a list of test suites.

You can perform the following actions on the test suites:

- **Upload** – Select **Upload**. A pop-up window appears. Select the desired test suite. The uploaded test suite will display in the test suite list in the Test Suite Manager interface. You can upload multiple test suites at one time. Before uploading the test suites, you must zip the test suites, and then select the ZIP file to upload them to Compliance Guardian Online.

  After you select **Upload**, if the checks with the same ID or same name as the ones you upload already exist in Compliance Guardian Online, or the test suites with the same name as the ones you upload already exist in Compliance Guardian Online, the **Upload** interface appears. All the checks with the same ID or name are displayed in the window, and all the test suites with the same name are displayed in the window. You can only select to upload the checks with the same ID and name and then select **Upload**, then the checks will replace the existing ones in Compliance Guardian Online. You can also select to upload the test suites, and then the test suites will overwrite the existing ones that have the same name.

  ***Note:** You can only upload a test suite if you have an enterprise license.

- **Download** – **Select Download** to download a selected test suite.

  ***Note**: You can only download a selected test suite if you have an enterprise license.

- **View** – Select **View** to view details about a selected test suite.
- **Edit** – Select the test suite that you want to edit, and then select **Edit**. For more information, refer to Editing Test Suite.
- **Delete** – Select any test suites you want to delete. You can only delete test suites that you uploaded to the Compliance Guardian Online Test Suite Manager.

Editing Test Suite

To edit a test suite, select the test suite, and then select **Edit**. A drop-down list appears. You can select to edit the test suite's basic settings or test suite's attributes.

***Note**: If you have a trial license, you can only edit the following built-in test suites: **Section 508**, **WCAG 2.0**, **Site Quality Report**, **Privacy Basics**, **Classification example** and **Redact Disallowed Words with Asterisk**. You cannot edit the other built-in test suites; if you have an enterprise license, you can edit all of the test suites.

Editing Basic Settings

Select **Edit Basic Settings** in the drop-down list. The Edit Basic Settings interface appears. Configure the following settings:

- **Name** – Edit the test suite name.
- **Description** – Edit the test suite description.

  ***Note**: You cannot edit a built-in test suite's name and description in the **Edit Basic Settings** interface.

- **Check Selection** – Select the checks that can be contained in this test suites by selecting or deselecting the checkboxes before the checks. Select **View** beside a check to view the detailed information on the check. If you have purchased the corresponding test suite group in your license, you can see **Edit** beside the check. Select **Edit** to go to the **Edit Chec**k interface. For more information on editing checks, refer to Editing Checks.

Select **Save** to save the changes. Select **Save As** to save the test suite to another one. At any time, select **Cancel** to return to the Test Suite Manager interface without any changes.

Editing Test Suite Attributes

Select **Edit Test Suite Attributes** in the drop-down list. The **Edit Test Suite Attributes** interface appears. There are two formats of the selected test suite displaying in the **Edit Test Suite Attributes** interface.

Under the **XML Format** tab, the test suite is displayed in the XML format. Refer to the following tips to edit the attributes:

- Double-click the attribute that you want to edit. The attribute is as editable. You can also double-click the entire row to make the attributes in the row editable.
- For some attributes, you can edit them directly in the editable text box. For other attributes, edit them by selecting another value in the drop-down list. If you want to change a check (edit the **tdfID** attribute), you can search the specified checks by entering a keyword in the search field in the drop-down list.
- To add a node, double-click the entire row under which you want to add the node. Then, press **Enter** on the keyboard. The new node is added. Enter the attributes in the newly added node according to your requirement.

- To delete a node, double-click the entire row, and then delete all of the content of this row.
- For details about the attributes of the test suite, refer to Test Suites.

Check Manager

Check Manager allows you to manage checks. To access **Check Manager** settings in the **Application Profiles** interface, select **Check Manager** under the **Application Profiles** heading.

Managing Checks

In the **Check Manager** interface, you will see a list of checks.

You can perform the following actions on the checks:

- **Upload** – Select **Upload**. A pop-up window appears. Select the desired check. The uploaded check will display in the check list in the Check Manager interface. You can upload multiple checks at one time. Before uploading the checks, you must zip the checks, and then select the ZIP file to upload them to Compliance Guardian Online.

  After you select **Upload**, if the checks with the same ID or same name as the ones you upload already exist in Compliance Guardian Online, the **Upload** interface appears. All the checks with the same ID or name are displayed in the window. You can only select to upload the checks with the same ID and name and then select **Upload**, then the checks will replace the existing ones in Compliance Guardian Online.

  ***Note:** You can only upload a check if you have an enterprise license.

- **Download** – Select **Download** to download a selected check.

  ***Note**: You can only download a selected check if you have an enterprise license.

- **View** – Select **View** to view details about a selected check.
- **Edit** – Select the check that you want to edit, and then select **Edit**. For more information, refer to Editing Checks.
- **Delete** – Select any checks you want to delete. You can only delete checks that you have uploaded to the Compliance Guardian Online Check Manager.

Editing Checks

To edit a check, select the check, and then select **Edit**. The **Edit Check** interface appears.

There are two formats of the selected check displaying in the **Edit Check** interface.

Under the **XML Format** tab, the check is displayed in the XML format. Refer to the following steps to edit the attributes:

- Double-click on the attribute that you want to edit. The attribute appears as editable. You can also double-click the entire row, then the attributes in the row are editable.
- You can edit some attributes directly in the editable text box. For other attributes, edit them by selecting another value in the drop-down list. If you want to change a check (edit the **cPIITdf** attribute), you can search the specified checks by entering a keyword in the search field in the drop-down list.
- To add a node, double-click the entire row under which you want to add the node. Then, press **Enter** on the keyboard. The new node is added. Enter the attributes in the newly added node according to your requirement.
- To delete a node, double-click the entire row, and then delete all of the content of this row.
- For details about the attributes of the check, refer to Checks.
- Press **Enter** on the keyboard or select on any other field of the interface to confirm the modification. Press **Esc** on the keyboard to cancel the modification.

Under the **Text** Format tab, the check is displayed in the text format. You can edit, add, or delete any of the attributes of the check. For details about the attributes about the check, refer to Checks.

Select **Save** to save the changes; Select **Save As** to save the check as another one. At any time, select **Cancel** to return to the Check Manager interface without any changes. If the edited check is used by some test suites, after you select **Save**, a pop-up window appears to display the test suites that are using the test suite. Select **OK** in the window to confirm the edit, or select **Cancel** in the window to cancel editing the check.

Filter Policy

Filter Policy allows you to set up filter rules so you can control what objects and data appear so that you can target content more precisely. By setting up and saving filter policies, you can apply the same filter policies in a spider profile for scanning webpages and SharePoint Online sites.

To access **Filter Policy** for Compliance Guardian Online in the Settings interface, select **Filter Policy** under the **Application Profiles** heading.

Managing Filter Policies

In the **Filter Policy** interface, you will see a list of previously configured filter policies.

You may perform any of the following actions on a selected filter policy:

- **Create** – Select **Create** to create a new filter policy. Refer to the Creating and Editing Filter Policies section for the details.
- **View** – Select **View** to see the details of the selected filter policy. Here you can also select **Edit** to make changes to the filter policy's settings. You will be brought to the **Edit** page where you can change the settings for this filter policy. After editing the settings,

select **Save** to save the changes, select **Save As** to save the filter policy as another one. At any time, select **Cancel** to return to the **Filter Policy** interface without saving any of your changes.

- **Edit** – Select **Edit** to make changes to the selected filter policy's settings. You will be brought to the **Edit** page where you can change the settings for this filter policy. Select **Save** to save the filter policy. To save a changed filter policy as a new one, select **Save As**. At any time, select **Cancel** to return to the **Filter Policy** without saving any of your changes.
- **Delete** – Select **Delete** to delete the selected filter policies. A warning message will appear to confirm the deletion. Select **OK** to delete the selected plan, or select **Cancel** to return to **Filter Policy** without deleting the selected filter policies.

Creating and Editing Filter Policies

Compliance Guardian Online provides three types of filter policies which can be used for scanning websites, scanning SharePoint Online sites, and taking actions on files. Refer to the following section for details.

Creating and Editing Filter Policies for Scanning Website

To create a new filter profile for scanning a website in Compliance Scanner, complete the following steps:

1. Select **Create** on the **Filter Policy** page.
2. Select **For Website** in the drop-down list. To modify a previously configured filter policy, select the filter policy, and then select **Edit**. The **Create Filter Policy** or **Edit Filter Policy** interface appears.
3. Configure the following settings:
    - **Name** – Enter a name for the filter policy.
    - **Description** – Enter a description for the filter policy (optional).
    - **Share Mode** – Select the share mode. If **Public** is selected, all users can see the filter policy you created. If **Private** is selected, only you can see the filter policy.
    - **Criteria** – Configure the criteria settings for the filter policy. Select **Add a Criterion** to add a new rule by completing the following fields:
        - **Rule** – Select the new rule you want to create from the drop-down list.
        - **Condition** – Select the condition for the rule.
        - **Value** – Enter a value you want the rule to use in the text box.

    ***Note:** Depending on the filters you enter, you can change the logical relationships between the filter rules. There are currently two logical relationships: **And** and **Or**. The logic is set to **And**. To change the logical relationship, select the logical relationship link. The **And** logical relationship means that the content which meets all of the rules will be

filtered and included in the result. The **Or** logic means that the content which meets any one of the rules will be filtered and included in the result.

You can view the logical relationship of the filter rules in the **Basic Filter Condition** area. For example, if the logical relationship is ((1 And 2) Or 3) in the **Basic Filter Condition** area, the contents that meet both the filter rule 1 and filter rule 2, or meet the filter rule 3, will be filtered out.

To add more filters, repeat the previous step.

Select **Remove** to delete a rule that is no longer needed.

4. Select **Save** to save the configurations and return to the **Filter Policy** interface. If you edit a filter policy, select **Save As** to save the filter policy to another one. At any time, select **Cancel** to return to the **Filter Policy** interface without saving any changes.

Creating and Editing Filter Policies for Scanning SharePoint Online Sites

To create a new filter profile for scanning SharePoint Online sites in Compliance Scanner and Classification Scanner, complete the following steps:

1. Select **Create** on the **Filter Policy** page.
2. Select **For SharePoint Online** in the drop-down list. To modify a previously configured filter policy, select the filter policy, and then select **Edit**. The **Create Filter Policy** or **Edit Filter Policy** interface appears.
3. Configure the following settings:
    - **Name** – Enter a name for the filter policy.
    - **Description** – Enter a description for the filter policy (optional).
    - **Share Mode** – Select the share mode. If **Public** is selected, all users can see the filter policy you created. If **Private** is selected, only you can see the filter policy.
    - **Criteria** – Configure the criteria settings for the filter policy. The criteria include Site Collection, Site, List/Library, Folder, Item, Document, Attachment and File Content. Select **Add a Criterion** to add a new rule by completing the following fields:
        - **Rule** – Select the new rule you want to create from the drop-down list.
        - **Condition** – Select the condition for the rule.
        - **Value** – Enter a value you want the rule to use in the text box.

    ***Note:** Depending on the filters you enter, you can change the logical relationships between the filter rules. There are currently two logical relationships: **And** and **Or**. The logic is set to **And**. To change the logical relationship, select the logical relationship link. The **And** logical relationship means that the content which meets all of the rules will be filtered and included in the result. The **Or** logic means that the content which meets any one of the rules will be filtered and included in the result.

You can view the logical relationship of the filter rules in the **Basic Filter Condition** area. For example, if the logical relationship is ((1 And 2) Or 3) in the **Basic Filter Condition** area, the contents that meet both the filter rule 1 and filter rule 2, or meet the filter rule 3, will be filtered out.

To add more filters, repeat the previous step.

Select **Remove** to delete a rule that is no longer needed.

4. Select **Save** to save the configurations and return to the **Filter Policy** interface. If you edit a filter policy, select **Save As** to save the filter policy to another one. At any time, select **Cancel** to return to the **Filter Policy** interface without saving any changes.

Creating and Editing Filter Policies for Taking Actions on Files

To create a new filter policy for determining the files to be taken actions in Classification Scanner, complete the following steps:

1. Select **Create** on the **Filter Policy** page.
2. Select **For Action Policy** in the drop-down list. To modify a previously configured filter policy, select the filter policy, and then select **Edit**. The **Create Filter Policy** or **Edit Filter Policy** interface appears.
3. Configure the following settings:
    - **Name** – Enter a name for the filter policy.
    - **Description** – Enter a description for the filter policy (optional).
    - **Share Mode** – Select the share mode. If **Public** is selected, all users can see the filter policy you created. If **Private** is selected, only you can see the filter policy.
    - **Criteria** – Configure the criteria settings for the filter policy. Select **Add a Criterion** to add a new rule by completing the following fields:
        - **Rule** – Select the new rule you want to create from the drop-down list.
        - **Condition** – Select the condition for the rule.
        - **Value** – Enter a value you want the rule to use in the text box.

      The filter rule contains three levels:

        - **Document** – Based on the SharePoint Document property value you specified here to define the scope in which the files will be affected by the specified actions.
        - **Item** – Based on the SharePoint Item property value you specified here to define the scope in which the items will be affected by the specified actions.
        - **Classification Result** – Based on the tag value you specified here to define the scope in which the files will be affected by the specified actions.

*__Note:__ Depending on the filters you enter, you can change the logical relationships between the filter rules. There are currently two logical relationships: **And** and **Or**. The logic is set to **And**. To change the logical relationship, select the logical relationship drop-down list. The **And** logical relationship means that the content which meets all of the rules will be filtered and included in the result. The **Or** logic means that the content which meets any one of the rules will be filtered and included in the result.

You can view the logical relationship of the filter rules in the **Basic Filter Condition** area.

To add more filters, repeat the previous step.

Select the checkbox before a rule, and then select **Remove** to delete a rule that is no longer needed.

4. Select **Save** to save the configurations and return to the **Filter Policy** interface. If you edit a filter policy, select **Save As** to save the filter policy to another one. At any time, select **Cancel** to return to the **Filter Policy** interface without saving any changes.

Action Policy

Classification Scanner is used to scan and classify content. The Action Policy takes the defined action (Move, delete, block, quarantine, encrypt, or redact) based on the result of the scan.

Managing Action Policies

The **Action Policy** interface displays all of the action policies that you have previously created.

Perform the following actions in the **Action Policy** interface:

- **Create** – Select **Create** on the ribbon to create a new action policy. For information about creating a new action policy, refer to Creating and Editing Action Policies.
- **View** – Select **View** on the ribbon and you will see the previously configured settings for the selected action policy. Here you can also select **Edit** on the ribbon to make changes to the action policy's settings. You will be brought to the **Edit Action Policy** interface where you can change this action policy.
- **Edit** – Select **Edit** on the ribbon to change the configurations for the selected action policy. For information about editing configurations for an action policy, refer to Creating and Editing Action Policies.
- **Delete** – Select **Delete** on the ribbon. A confirmation window will appear and ask if you are sure you want to proceed with the deletion. Select **OK** to delete the selected action policies, or select **Cancel** to return to the **Action Policy** interface without deleting the selected action policies.

Creating and Editing Action Policies

To create a new action, complete the following steps:

1. Select **Create** on the **Action Policy** page. To modify a previously configured action policy, select the action policy, and then select **Edit**. The **Create Action Policy** or **Edit Action Policy** interface appears.
2. Enter a Name for the action policy, and enter an optional Description for future reference. Then, configure the **Set up the scan action rules** section:
    - **Conditions** – Select a filter policy that is used for the action policy from the drop-down list. For more information on configuring the filter policy used for the action policy, refer to Creating and Editing Filter Policies for Taking Actions on Files.
    - **Actions** – Select an action to handle the files. Then select **Add an action**.

      Repeat the above step to add multiple actions. The actions then will be added. If the **Configure** button appears after the added action, you must select it to configure the settings for the action. Select the delete ( ) button after an action to deselect to add this action. You can change the order of the action configuration by selecting the textbox before the added action to determine the priority of the action. For details of each action, refer to Classification Actions.
    - **Alert** – Specify whether to send an e-mail when the action fails to execute or successfully executes to the scanned files, and then select an alert profile.

    Select **Add a Condition Group** to add another condition group. Select the delete ( ) button after a condition group to delete the condition group. You can change the order of the condition group configuration by selecting the textbox on the top of each condition group to determine the priority of the condition group. Select the right arrow ( ) or down arrow ( ) to expand or retract the settings of a condition group.
3. Select **Save** to save the settings, or select **Cancel** to return to the Action Policy interface without saving any changes. If you are editing the action policy, you can save the action policy as another one by selecting **Save As**.

Classification Actions

Refer to the following section for details about each classification action.

Change Permission

The permissions of the files or items filtered based on the Conditions setting will be changed based on your settings. When selecting **Configure** after the **Change Permission** action in the Create Action Policy or Edit Action Policy interface, configure the following settings in the **Configure Change Permission** field:

- **SharePoint Group Name** – Enter a group name. If the group does not exist, it will be created.
- **Group Permissions** – Specify permissions for the group. Users in the group will have the specified permissions to the files or items. If the group exists in SharePoint Online, the original group permissions will not be changed although you specify permissions here.

Delete Files/Items

The files or items filtered based on the Conditions setting will be deleted to the Recycle Bin.

Encrypt

The files or items filtered based on the Conditions setting will be encrypted. After you select **Configure** after the **Encrypt** action in the Create Action Policy or Edit Action Policy interface, configure the following settings in the **Configure Encrypt** field:

- **Security Profile** – Select a security profile for encrypting the files or items. Select **New Security Profile** to create a new security profile. For more information, refer to Security Profile.

Encrypt and Quarantine

The files or items filtered based on the Conditions setting will be encrypted and then quarantined. After you select **Configure** after the **Encrypt and Quarantine** action in the Create Action Policy or Edit Action Policy interface, configure the following settings in the **Configure Encrypt and Quarantine** field:

- **Quarantine Method** – Select a Quarantine Method.
  - **In place quarantine** – The files or items will be quarantined, but they are still in SharePoint Online.
    - **Specify a SharePoint group that has permission to view or manage the encrypted data in SharePoint** – Enter a group name, and then specify permissions for the group. The users in the group will have the specified permissions to the files or items whose Quarantine Method is **In place quarantine**.

      ***Note**: If the group does not exist in SharePoint Online, the new group will be created. If the group already exist in SharePoint Online, the group permissions will not be changed although you specify permissions here
  - **Out of place quarantine** – The files or items will be quarantined to the Azure storage.
- **Security Profile** – Select a security profile for encrypting the files or items. Select **New Security Profile** to create a new security profile. For more information, refer to Security Profile.

Move to the Allowed Location

The scanned files filtered based on the Conditions setting will be moved to the allowed location configured below.

***Note**: Only the files in the document library can be moved.

You must first configure the location where the file will move. Select the **Configure Location Settings** link after **Move to the Allowed Location**, the **Location Settings** field appears. Configure the following settings:

- **Move to the library or folder in other site** – Select this radio button and complete the following step to select a destination location:
    i. Select an authentication profile used to connect to Office 365 admin center.
    ii. Select **My Registered Sites**. The Compliance Guardian Online will connect to Office 365 admin center and scan all of the site collections using the account entered in the selected authentication profile. Then, all of the SharePoint Online site collections will be listed under the **My Registered Sites** node.
    iii. Expand the desired site collection and then select library or folder as the destination to store the moved files.
- **Move to the library or folder in the same site** – Select the radio button, and then enter the path of the library or folder you want to move the files to.

Select **Save** to save the location settings.

After you configure the location, you can configure the Advanced settings to define whether or not to move the files that failed to be moved. Select the **Advanced Settings** link after **Move to the Allowed Location**, the Advanced Settings field appears. Select the **If the files fail to move, they will be quarantined** checkbox if you want to deal with the files that failed to be moved. With this option enabled, the files will be quarantined. The following conditions will lead to the failure:

- There is no content type that matches the source file's content type in the target library.
- The matched content type of the target library (where the allowed location is) does not contain all of the source file's columns.
- There is a file in the destination library or folder whose name is same as the file that will be moved.
- Other unknown system issues.

If the **If the files fail to move, they will be quarantined** checkbox is selected, configure the following Quarantine Method:

- **In place quarantine** – The files will be quarantined, but they are still in SharePoint Online.
    - **Specify a SharePoint group that has the permission to view or manage the quarantined data in SharePoint** – Enter a group name, and then specify permissions for the group. The users in the group will have the specified permissions to the files or items whose Quarantine Method is **In place quarantine**.

      ***Note**: If the group does not exist in SharePoint Online, the new group will be created; If the group already exist in SharePoint Online, the group permissions will not be changed although you specify permissions here.
- **Out of place quarantine** – The files will be quarantined to the Azure storage.

Permanently Delete
The Newsfeed and the replies of the Newsfeed filtered based on the Conditions setting will be permanently deleted.

Quarantine Files/Items
The files or items filtered based on the Conditions setting will be quarantined.

After you select **Configure** after the **Quarantine Files/Items** action in the Create Action Policy or Edit Action Policy interface, configure the Quarantine Method settings in the **Configure Quarantine Files/Items** field.

- **In place quarantine** – The files or items will be quarantined, but they are still in SharePoint Online. The users in the groups selected in the **Specify a SharePoint group that has permission to view or manage the quarantined data in SharePoint Online** field can view or manage these quarantined files or items.
    - **Specify a SharePoint group that has the permissions to view or manage the quarantined data in SharePoint –** Enter a group name, and then specify permissions for the group. The users in the group will have the specified permissions to the files or items whose Quarantine Method is **In place quarantine**.

      ***Note**: If the group does not exist in SharePoint Online, the new group will be created. If the group already exist in SharePoint Online, the group permissions will not be changed although you specify permissions here.
- **Out of place quarantine** – The files or items will be quarantined to the Azure storage.

Redact Files/Items
Redact the files or items filtered based on the Conditions setting according to the Redaction type test suite. After you select **Configure** after the **Redact Files/Items** action in the Create Action Policy or Edit Action Policy interface, the **Configure Redact Files/Items** field appears. Then, select a Redaction type test suite to redact the files or items.

Quarantine Before Redact
The files or items filtered based on the Conditions setting will be backed up, and the backed up files or items will be quarantined. The original files or items in SharePoint will be redacted. After you select **Configure** after the **Quarantine Before Redact** action in the Create Action Policy or Edit Action Policy interface, the **Configure Quarantine Before Redact** field appears. Then, select a Redaction type test suite to redact the files or items.

User Agent Profile

A user agent profile is used for the backend web server when scanning the website. To configure user agent profiles in the **Settings** interface, select **User Agent Profile** under the **Application Profiles** heading.

Managing User Agent Profiles

In the **User Agent Profile** interface, you will see a list of previously configured user agent profiles.

You may perform any of the following actions on a selected user agent profile:

- **Create** – Select **Create** to create a new user agent profile. Refer to the Creating and Editing User Agent Profiles section for the details.
- **View** – Select **View** to see the details of the selected user agent profile. Here you can also select **Edit** to make changes to the profile's settings. You will be brought to the **Edit** page where you can change the settings for this profile. After editing the settings, select **Save** to save the changes, select **Save As** to save the profile as another one. At any time, select **Cancel** to return to the **User Agent Profile** interface without saving any of your changes.
- **Edit** – Select **Edit** to make changes to the selected profile's settings. You will be brought to the **Edit** page where you can change the settings for this profile. Select **Save** to save the scan. To save a changed user agent profile as a new one, select **Save As**. At any time, select **Cancel** to return to the **User Agent Profile** without saving any of your changes.
- **Delete** – Select **Delete** to delete the selected profiles. A warning message will appear to confirm the deletion. Select **OK** to delete the selected plan, or select **Cancel** to return to **User Agent Profile** without deleting the selected user agent profiles.

Creating and Editing User Agent Profiles

To create a new user agent profile, select **Create** in the **Manage** group of the User Agent Profile page. To modify a previously configured user agent profile, select the user agent profile, and then select **Edit** on the ribbon. In the Create User Agent Profile or Edit User Agent Profile interface, configure the following settings:

- **Name** – Enter a name for the user agent profile.
- **Description** – Enter a description for the user agent profile (optional).
- **Share Mode** – Select the share mode. If **Public** is selected, all users can see the user agent profile you created; if **Private** is selected, only you can see the user agent profile.
- **User Agent String** – Specify the user agent string. The user agent string is the text that programs use to identify themselves to HTTP, mail, and news servers for usage tracking purposes. For more information about user agent strings, refer to Microsoft's "Understanding user-agent strings" article.

Select **Save** to save the configurations and return to the **User Agent Profile** interface. If you edit a user agent profile, select **Save As** to save the profile to another one. At any time, select **Cancel** to return to the **User Agent Profile** interface without saving any changes.

Authentication Profile

An authentication profile is used to connect to the website or SharePoint Online sites. To configure authentication profiles in the **Settings** interface, select **Authentication Profile** under the **Application Profiles** heading.

Managing Authentication Profiles

In the **Authentication Profile** interface, you will see a list of previously configured authentication profiles.

You may perform any of the following actions on a selected authentication profile:

- **Create** – Select **Create** to create a new authentication profile. Refer to the Creating and Editing Authentication Profiles section for the details.
- **View** – Select **View** to see the details of the selected authentication profile. Here you can also select **Edit** to make changes to the profile's settings. You will be brought to the **Edit** page where you can change the settings for this profile. After editing the settings, select **Save** to save the changes, select **Save As** to save the profile as another one. At any time, select **Cancel** to return to the **Authentication Profile** interface without saving any of your changes.
- **Edit** – Select **Edit** to make changes to the selected profile's settings. You will be brought to the **Edit** page where you can change the settings for this profile. Select **Save** to save the scan. To save a changed authentication profile as a new one, select **Save As**. At any time, select **Cancel** to return to the **Authentication Profile** without saving any of your changes.
- **Delete** – Select **Delete** to delete the selected profiles. A warning message will appear to confirm the deletion. Select **OK** to delete the selected plan, or select **Cancel** to return to **Authentication Profile** without deleting the selected authentication profiles.

Creating and Editing Authentication Profiles

Compliance Guardian Online provides two type of authentication profiles, which can be used to scan websites and SharePoint Online sites. Refer to the following section for details.

Creating and Editing Authentication Profiles for Scanning Website

To create a new authentication profile for scanning website, complete the following steps:

1. Select **Create** in the **Authentication Profile** page. Then, select **For Website** in the drop-down list. To modify a previously configured authentication profile, select the authentication profile, and

then select **Edit**. The **Create Authentication Profile** or **Edit Authentication Profile** interface appears.

2. Configure the following settings:
    - **Name** – Enter a name for the authentication profile.
    - **Description** – Enter a description for the authentication profile (optional).
    - **Share Mode** – Select the share mode. If **Public** is selected, all users can see the authentication profile you created; if **Private** is selected, only you can see the authentication profile.
    - **Authentication Method** – Select one of the following authentication methods:
        - **Username and Password** – If this method is selected, then enter the specified username and password to access the website.
        - **Certificate** – If this method is selected, upload a certificate, and then specify the username and password to access the website.
        - **SharePoint Online** – This method is only used for scanning the SharePoint Online sites. If this method is selected, then enter the username and password to access the SharePoint Online site.
        - **Form-Based Authentication** – This method is used for scanning the website that can be logged in after filling in the form and submitting the filled information. You are required to enter the following information after selecting **Form-Based Authentication:**
            - **Login URL** – Enter the form URL.
            - **Username Class or ID** – Enter the login username class or ID.
            - **Username** – Enter the login username.
            - **Password Class or ID** – Enter the login password class or ID.
            - **Password** – Enter the login password.
            - **Login Button Class or ID** – Enter the login button class or ID.
3. Select **Save** to save the configurations and return to the **Authentication Profile** interface. If you edit an authentication profile, select **Save As** to save the profile to another one. At any time, select **Cancel** to return to the **Authentication Profile** interface without saving any changes.

Creating and Editing Authentication Profiles for Scanning SharePoint Online Sites

To create a new authentication profile for scanning SharePoint Online sites, complete the following steps:

1. Select **Create** in the Authentication Profile page.
2. Select **For SharePoint Online** in the drop-down list. To modify an authentication profile, select the authentication profile, and then select **Edit**. The **Create Authentication Profile** or **Edit Authentication Profile** interface appears.

3. Configure the following settings:
    - **Name** – Enter a name for the authentication profile.
    - **Description** – Enter a description for the authentication profile (optional).
    - **Share Mode** – Select the share mode. If **Public** is selected, all users can see the authentication profile you created; if **Private** is selected, only you can see the authentication profile.
    - **Office 365 Account** – Configure the authentication settings:
        - **Username** – Enter the username that is used to connect to the Office 365 admin center.
        - **Password** – Enter the password that is used to connect to the Office 365 admin center.
        - **SharePoint Admin Center URL** – The URL of the SharePoint admin center site.
4. Select **Save** to save the configurations and return to the **Authentication Profile** interface. If you edit an authentication profile, select **Save As** to save the profile to another one. At any time, select **Cancel** to return to the **Authentication Profile** interface without saving any changes.

User Notification Profile

Compliance Guardian Online offers e-mail reports or notifications to provide you with information about a scan.

To access the User Notification Profile for Compliance Guardian Online, navigate to the **Settings** interface, and then select **User Notification Profile** under the **Application Profiles** heading.

Managing User Notification Profile

In the **User Notification Profile** interface, you will see a list of previously configured notification profiles.

You may perform any of the following actions on a selected user notification profile:

- **Create** – Select **Create** to create a new authentication profile. Refer to the Creating and Editing User Notification Profile section for the details.
- **View** – Select **View** to see the details of the selected user notification profile. Here you can also select **Edit** to make changes to the profile's settings. You will be brought to the **Edit** page where you can change the settings for this profile. After editing the settings, select **Save** to save the changes, select **Save As** to save the profile as another one. At any time, select **Cancel** to return to the **User Notification Profile** interface without saving any of your changes.
- **Edit** – Select **Edit** to make changes to the selected profile's settings. You will be brought to the **Edit** page where you can change the settings for this profile. Select **Save** to save the scan. To save a changed notification profile as a new one, select **Save As**. At any

time, select **Cancel** to return to the **User Notification Profile** without saving any of your changes.

- **Delete** – Select **Delete** to delete the selected profiles. A warning message will appear to confirm the deletion. Select **OK** to delete the selected profiles, or select **Cancel** to return to **User Notification Profile** without deleting the selected user notification profiles.

Creating and Editing User Notification Profile

To create a new authentication profile, select **Create** on the **User Notification Profile** page. To modify a user notification profile, select the user notification profile, and then select **Edit**. In the Create User Notification Profile or Edit User Notification Profile interface, configure the following settings:

- **Name** – Enter a name for the authentication profile.
- **Description** – Enter a description for the authentication profile (optional).
- **Share Mode** – Select the share mode. If **Public** is selected, all users can see the authentication profile you created; if **Private** is selected, only you can see the authentication profile.
- **Format** – Select the format of the e-mail that will be sent.
- **Recipients** – Specify the recipients that will receive the e-mail. Use the semicolon (**;**) as a separator if multiple recipients are specified.

Select **Save** to save the configurations and return to the **User Notification Profile** interface. If you edit a user notification profile, select **Save As** to save the profile to another one. At any time, select **Cancel** to return to the **User Notification Profile** interface without saving any changes.

Alert Profile

An alert profile is used to configure the alert e-mail settings. The alert e-mail can be sent when a file fails to be scanned, a file fails to be add tag, there is a violation found in the file, etc.

To access the Alert Profile for Compliance Guardian Online, navigate to the **Settings** interface, and then select **Alert Profile** under the **Application Profiles** heading.

Managing Alert Profiles

In the **Alert Profile** interface, you will see a list of alert profiles.

You may perform any of the following actions on a selected alert profile:

- **Create** – Select **Create** to create a new alert profile. Refer to Creating and Editing Alert Profiles.
- **View** – Select **View** to see the details of the selected alert profile. Here you can also select **Edit** to make changes to the profile's settings. You will be brought to the **Edit** page where you can change the settings for this profile. After editing the settings, select **Save**

to save the changes, select **Save As** to save the profile as another one, or select **Cancel** to return to the **Alert Profile** interface without saving any of your changes.

- **Edit** – Select **Edit** to make changes to the selected profile's settings. You will be brought to the **Edit** page where you can change the settings for this profile. Select **Save** to save the profile. To save a changed alert profile as a new one, select **Save As**. At any time, select **Cancel** to return to the **Alert Profile** without saving any of your changes.
- **Delete** – Select **Delete** to delete the selected profiles. A warning message will appear to confirm the deletion. Select **OK** to delete the selected profiles, or select **Cancel** to return to **Alert Profile** without deleting the selected profiles.

Creating and Editing Alert Profiles

To create or edit a new alert profile, complete the following steps:

1. Select **Create** in the **Alert Profile** page. To modify an alert profile, select the alert profile, and then select **Edit**. The Create Alert Profile or Edit Alert Profile interface appears.
2. Configure the following settings:
    - **Name** – Enter a name for the alert profile.
    - **Description** – Enter a description for the alert profile (optional).
    - **Share Mode** – Select the share mode. If **Public** is selected, all users can see the alert profile you created; if **Private** is selected, only you can see the alert profile.
    - **Recipients** – Specify the recipients that will receive the e-mail.
        - **Creator** – The alert will send to the creator of the file, and then select the corresponding e-mail template.
        - **Modifier** – The alert will send to the modifier of the file, and then select the corresponding e-mail template.
        - **Specify alert address** – Enter the address of the recipients who will receive the alert.
            - **E-mail address** – If the **E-mail address** radio button is selected, select **Add an E-mail Address**, enter a recipient's e-mail address in the **E-mail Address** column, and then select a corresponding e-mail template. Select **Add an E-mail Address** again to add another recipient. Select **Remove** to delete a recipient.
            - **SharePoint group** – If the **SharePoint group** button is selected, select **Add a SharePoint Group**, enter a SharePoint group name in the **SharePoint Group** column, and then select a corresponding e-mail template. Select **Add a SharePoint Group** again to add another group. Select the **Remove** to delete a group.
3. Select **Save** to save the configurations and return to the **Alert Profile** interface. If you edit an alert profile, select **Save As** to save the profile to another one. At any time, select **Cancel** to return to the **Alert Profile** interface without saving any changes.

Security Profile

Security profile can protect your backup data using the security keys generated by the specified encryption method. In the **Security Profile** pane, there is a default security profile named **Default Security Profile**. The default profile is not able to be edited or deleted.

Profile Setting

To create a new security profile, select **Create**, and then configure the following settings:

- **Name** – Enter a profile name and an optional **Description**. When configuring encryption options while creating scans, security profile names are listed for you to select.
- **Share Mode –** Select the share mode. If Public is selected, all users can see the profile you created; if Private is selected, only you can see the profile.
- **Encryption Method** – Select encryption method and encryption length to be used in the encryption.
    - **Specify an encryption method** – Select an encryption method in the drop-down list from **AES**, **DES** and **Blowfish**.
    - **Encryption Length (bit)** – Specify the length of the encryption.
- **Encryption Key** – Select the way to generate an encryption key.
    - **Automatically generate an encryption Key** – Compliance Guardian Online will generate a key for you.
    - **Generate encryption Key from seed** – Select this option to have Compliance Guardian Online generate a key based on the seed you enter. If you choose this method, enter a seed into the **Seed** text box and then enter the same seed into the **Confirm seed** text box.

Select **Save** to save these configurations and return to the **Security Profile** interface, or select **Cancel** to return to the **Security Profile** interface without saving these configurations. The encryption method or length of a security profile cannot be modified once the profile has been created.

In the **Security Profile** interface, to modify the description and configuration for a previously configured security profile, select the profile you want to modify, and then select **Edit**. To delete a previously configured security profile, select the profile you want to delete, and then select **Delete**.

***Note:** If the security profile you want to delete is already in use, it is not allowed to be deleted.

E-mail Template

E-mail Template allows you to configure an e-mail template for the notifications and alerts.

To access the **E-mail Template** for Compliance Guardian Online, navigate to the **Settings** interface, and then select **E-mail Template** under the **Application Profiles** heading.

Managing E-mail Templates

In the **E-mail Template** interface, you will see a list of previously configured e-mail templates.

You may perform any of the following actions on a selected e-mail templates:

- **Create** – Select **Create** to create a new e-mail templates. Refer to Creating and Editing E-mail Templates.
- **View** – Select **View** to see the details of the selected e-mail template. Here you can also select **Edit** to make changes to the template's settings. You will be brought to the **Edit** page where you can change the settings for this template. After editing the settings, select **Save** to save the changes, select **Save As** to save the template as another one, or select **Cancel** to return to the **E-mail Template** interface without saving any of your changes.
- **Edit** – Select **Edit** to make changes to the selected template's settings. You will be brought to the **Edit** page where you can change the settings for this template. Select **Save** to save the template. To save a changed template as a new one, select **Save As**. At any time, select **Cancel** to return to the **E-mail Template** without saving any of your changes.
- **Delete** – Select **Delete** to delete the selected templates. A warning message will appear to confirm the deletion. Select **OK** to delete the selected profiles, or select **Cancel** to return to **E-mail Template** without deleting the selected templates.

Creating and Editing E-mail Templates

To create or edit a new e-mail template, complete the following steps:

1. Select **Create** in the **E-mail Template** page. To modify an e-mail template, select the e-mail template, and then select **Edit**. The Create E-mail Template or Edit E-mail Template interface appears.
2. Configure the following settings:
    - **Name** – Enter a Name for this e-mail template.
    - **Description** – Enter an optional description for this e-mail template.
    - **Share Mode** – Select the share mode. If **Public** is selected, all users can see the e-mail template you created; if **Private** is selected, only you can see the e-mail template.
    - **E-mail Template** – Specify the Subject and Body of the e-mail template. There are three columns that can be added to the e-mail subject: Item Name, Item URL and Scanned Time. There are seven columns that can be added to the e-mail body: Job ID, Scan Name, Job Type, Item Name, Item URL, Scanned Time and Reason. The values of these columns will be displayed in the e-mail is the columns are added in the e-mail template. Alternatively, you can customize the subject and body of the e-mail template with the desired content.

3. Select **Save** to save the configurations and return to the E-mail Template interface. If you edit an e-mail template, select **Save As** to save the template to another one. At any time, select **Cancel** to return to the E-mail Template interface without saving any changes.

Compliance Scanner

Compliance Scanner allows you to scan webpages or SharePoint Online sites using the defined rule. The corresponding compliance reports will be generated for the user to review.

Getting Started

Refer to the sections below for important information on getting started with Compliance Scanner.

Launching Compliance Scanner

To launch Compliance Scanner, complete the following steps:

1. Log into Compliance Guardian Online.
2. Select **Compliance Scanner** to launch its interface.
3. If you are already in the software, select **Scanner** on the top of the interface, and then select **Compliance Scanner** from in the drop-down list.

Managing Scans

In the **Compliance Scanner** interface, you will see a list of scans.

You may perform any of the following actions on a selected scan:

- **Create** – Select **Create** to create a new scan. Refer to the Creating Scans section for the details.
- **View** – Select **View** to see the details of the selected scan. In the View Scan interface, select **Scan Now** to scan immediately. Here you can also select **Edit** to make changes to the scan's settings. You will be brought to the **Edit** page where you can change the settings for this scan. After editing the settings, select the down arrow (⌄) after **Save**, a drop-down list appears. Select **Save** in the drop-down list to save the changes; to save a changed scan as a new one, select **Save As**; select **Save and Scan Now** in the drop-down list to save the scan and run immediately. At any time, select **Cancel** to return to the **Compliance Scanner** interface without saving any of your changes.
- **Edit** – Select **Edit** to make changes to the selected scan's settings. You will be brought to the **Edit** page where you can change the settings for this scan. Select the down arrow (⌄) next to **Save**. A drop-down list appears. Select **Save** in the drop-down list to save the changes; to save a changed scan as a new one, select **Save As**; select **Save and Scan Now** in the drop-down list to save the scan and run immediately. At any time, select **Cancel** to return to the **Compliance Scanner** without saving any of your changes.
- **Delete** – Select **Delete** to delete the selected scans. A warning message will appear to confirm the deletion. Select **OK** to delete the selected plan, or select **Cancel** to return to **Compliance Scanner** interface without deleting the selected scans.

- **Scan** – Run the selected scan immediately.

Creating Scans

Refer to the following section for creating a scan.

Creating Scans to Scan Website

To create a new scan for scanning websites, select **Create**, and then select **For Website** in the drop-down list. In the **Create Scan** interface, configure the following settings:

- **Start From** – Enter a URL. Compliance Guardian Online scans the objects from this URL. Optionally, you can select to use the Compliance Guardian Online Transaction Capture tool to save a transaction file, and select the **Use Compliance Guardian Online Transaction Capture. Export the following transaction file for the scan** radio button in this interface to import a transaction file. The recorded URLs in the transaction file will be the start URLs. You can select **Download Compliance Guardian Online Transaction Capture** to download the Compliance Guardian Online Transaction Capture tool. For more information on the Compliance Guardian Online Transaction Capture tool, refer to Appendix B: Using Compliance Guardian Online Transaction Capture.
- **Maximum Pages** – Specify the maximum pages allowed to crawl in a single job. If you have a trial license, you can specify 100 at most; if you have an enterprise license, you can scan all the pages of an entire website. Enter **unlimited** if you want to scan all the pages of an entire website.
- **Test Suite Selection** – Select the test suites from the drop-down list. You can search the test suites by entering a keyword in the search field in the drop-down list. The webpages will be scanned according to the rules defined in the selected test suites.
- **Spider Profile** – Select the spider profile. The webpages will be crawled based on the rules defined in the spider profile. Select **View** to view the settings in the selected spider profile. Select **Edit** to edit the spider profile. For the details about the spider profile, refer to Spider Profile.

Select **Save** to save the scan. After you select **Save**, a pop-up window appears. Then specify a scan name, and select the Share Mode. **Public** means that all users can see the scan you created. **Private** means that only you can see the scan. Select **Save** on the window to save the scan, and then you can view the scan in the Compliance Scanner page; select **Save and Scan Now** to scan the defined webpages immediately; Select **Cancel** to return to the Create Scan page.

Select **Scan Now** to scan the defined webpages immediately. You can go to Job Monitor to view the job details. The instant scan will not be displayed in the Compliance Scanner interface.

Select **Reset** to ease the settings you configured.

Select **Cancel** to return to the Compliance Scanner interface.

Creating Scans to Scan SharePoint Online Sites

To create a new scan for scanning SharePoint Online sites, select **Create**. Then, select **For SharePoint Online** in the drop-down list. The Create Scan interface appears.

***Note**: If you have a trial license, the maximum number of SharePoint Online items that can be scanned in one scan is 100.

Selecting Authentication Profile

You must first select an authentication profile to connect to the Office 365 admin center. In the upper-left corner of the Create Scan interface, select an authentication profile from the **Select an Authentication Profile** drop-down list. Select **Refresh** to refresh the authentication profile in the drop-down list.

Defining the SharePoint Online Site Scope

There are two methods for getting the SharePoint Online Site scope:

- **Automatically Discover SharePoint Online Sites** – Select this radio button in the left pane of the Create Scan interface, and then select **My Registered Sites**. Compliance Guardian Online will connect to Office 365 admin center and scan all of the site collections using the account specified in the selected authentication profile. Then, all of the SharePoint Online site collections will be listed under the **My Registered Sites** node.

  ***Note**: If **Automatically Discover SharePoint Online Sites** is selected, the user in the selected authentication profile must have the site collection administrator permission to the target site collections, must have the Global administrator role, and the user must apply a valid SharePoint Online license.

- **Manually Enter SharePoint Online Site** – Select this radio button in the left pane of the Create Scan interface, a text box appears. Enter a SharePoint Online site collection and then select **My Registered Sites** node, the entered site collection is displayed under the **My Registered Sites** node.

  ***Note**: The entered site collection must exist in the connected Office 365 admin center.

  If **Manually Enter SharePoint Online Site** is selected, the user in the selected authentication profile must have the site collection administrator permission to the target site collections, and must apply a valid SharePoint Online license.

After getting the SharePoint Online sites, select the SharePoint Online site collection that you want to scan under the **My Registered Sites** node. You can also select the nodes under the site collection to scan.

If you want to scan the posts and replies in Newsfeed, you must select the **MicroFeed** list under a site.

If you want to scan the user profile, select the personal site collection, and deselect the top-level site node and the nodes under the top-level site node.

Configuring Scan Settings

In the right pane of the Create Scan interface, configure the following settings:

- **Test Suite Selection** – Select the test suites. The SharePoint Online sites will be scanned according to the rules defined in the selected test suites.
- **Spider Profile** – Select the spider profile used for Compliance Scanner. The SharePoint Online sites will be crawled based on the rules defined in the spider profile. Select **View** to view the settings in the selected spider profile. Select **Edit** to edit the spider profile. For the details about the spider profile, refer to Spider Profile.

Select **Save** to save the scan. A pop-up window appears. Enter the Scan Name and Share Mode, then you can save the scan by selecting **Save** in the window; select **Save and Scan Now** to save the scan and scan immediately; select **Cancel** to exit the window without any changes.

Select **Scan Now** to scan immediately.

Select **Reset** to erase any of the configured settings in the Create Scan interface.

Select **Cancel** to exit the Create Scan interface without any changes.

Editing Scans

To modify a previously configured scan, select the scan, and then select **Edit**. For more information about editing configurations for a scan, refer to Creating Scans.

Select **Save**. A drop-down list appears. Choose from the following options:

- Select **Save** from the drop-down list to save the changes.
- Select **Save As** to save the scan as another one.
- Select **Save and Scan Now** to save the changes and scan immediately.

Compliance Reports

Compliance Reports is used to record the scan results and display the reports including Risk Report, Data Table Report, File Errors Report, File Type Report, PDF Exception Report, Violation Report, Link Validation Report, Page Title Report, and Human Auditor report. It is also supported exporting the report to a datasheet or HTML file for your reference.

Launching Compliance Reports

To launch Compliance Reports, complete the following steps:

1. Log into Compliance Guardian Online.
2. In the home page of Compliance Guardian Online, select **Compliance Reports** to launch its interface.
3. Alternatively, select **Reports** on the top of the screen, a navigation bar appears.
4. Select the report page on the navigation bar to enter the desired report page.

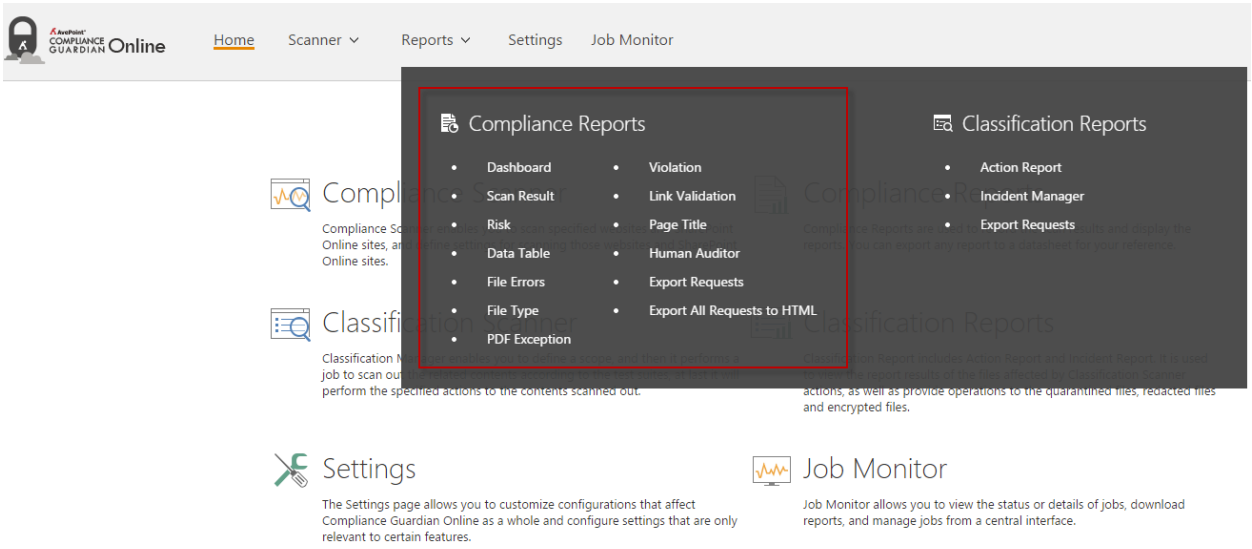

Figure 2: Compliance Reports navigation bar.

Getting Started

To get started in Compliance Reports, complete the following steps:

1. Select **Scan Filter** at the top-right corner of the page. A drop-down list appears.
2. Choose a scan from the drop-down list that containing the scan results you want to view. The scan results of the latest scan cycles of the scan will be displayed in different kinds of compliance reports in the Compliance Reports module.

3. If you want to save your selection as default, select the desired scan, and then select the **Save As Default** ( ) button after the scan. The next time you login to Compliance Reports, the scan results of the desired scan will be displayed.
4. If you want to delete a scan's related reports, select the **Delete** ( ) button after the scan. A confirmation window appears.
5. Select **OK** in the window to delete all of the scan's related reports, select **Cancel** without deleting any reports.

***Note**: After the scan has been selected, Compliance Guardian Online will use the same configured scan when displaying the search results in the interfaces of different compliance reports.

***Note**: Only the users in the defined Report Group have permissions to view the compliance reports of the corresponding scans.

Compliance Report Home Page

The Compliance Report home page provides the users with an overall view of the scan results in four areas:

- Scan Result Overview
- Risk Report Overview
- Violation Report Overview
- Other Reports Overview

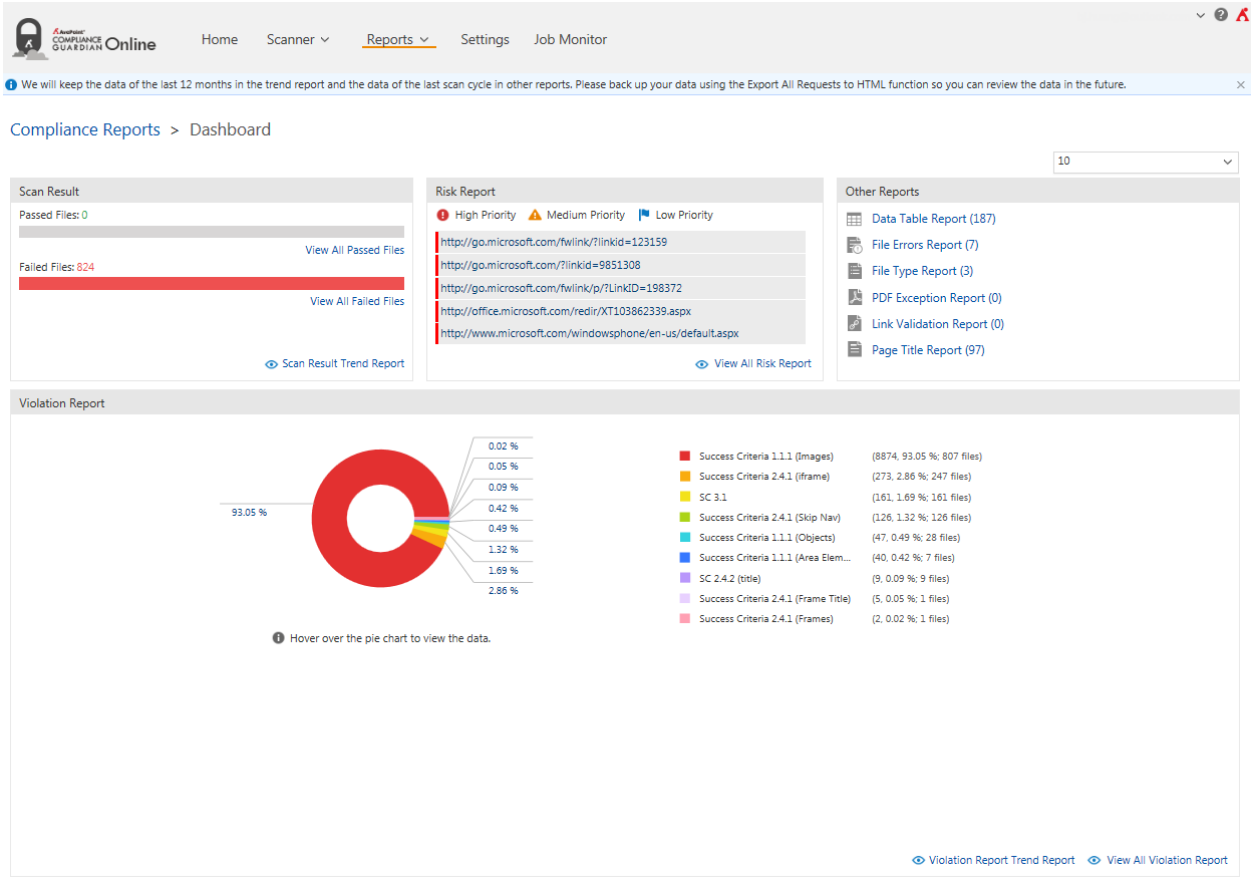
Compliance Guardian Online
Home
Scanner
Reports
Settings
Job Monitor
We will keep the data of the last 12 months in the trend report and the data of the last scan cycle in other reports. Please back up your data using the Export All Requests to HTML function so you can review the data in the future.
Compliance Reports > Dashboard
Scan Result
Passed Files: 0
View All Passed Files
Failed Files: 824
View All Failed Files
Scan Result Trend Report
Risk Report
High Priority
Medium Priority
Low Priority
http://go.microsoft.com/fwlink/?linkid=123159
http://go.microsoft.com/?linkid=9851308
http://go.microsoft.com/fwlink/p/?LinkID=198372
http://office.microsoft.com/redir/XT103862339.aspx
http://www.microsoft.com/windowsphone/en-us/default.aspx
View All Risk Report
Other Reports
Data Table Report (187)
File Errors Report (7)
File Type Report (3)
PDF Exception Report (0)
Link Validation Report (0)
Page Title Report (97)
Violation Report
93.05 %
0.02 %
0.05 %
0.09 %
0.42 %
0.49 %
1.32 %
1.69 %
2.86 %
Success Criteria 1.1.1 (Images) (8874, 93.05 %; 807 files)
Success Criteria 2.4.1 (iframe) (273, 2.86 %; 247 files)
SC 3.1 (161, 1.69 %; 161 files)
Success Criteria 2.4.1 (Skip Nav) (126, 1.32 %; 126 files)
Success Criteria 1.1.1 (Objects) (47, 0.49 %; 28 files)
Success Criteria 1.1.1 (Area Elem... (40, 0.42 %; 7 files)
SC 2.4.2 (title) (9, 0.09 %; 9 files)
Success Criteria 2.4.1 (Frame Title) (5, 0.05 %; 1 files)
Success Criteria 2.4.1 (Frames) (2, 0.02 %; 1 files)
Hover over the pie chart to view the data.
Violation Report Trend Report
View All Violation Report

Figure 3: Compliance Reports page.

Scan Result Overview

The Scan Result overview area displays the histogram of the passed files and failed files analyzed by the scan engine. The total number of the passed and failed files is the number of all the files that have been analyzed by the scan engine.

- **Passed Files** – The files that meet the defined scan policy. Select **View All** to go to the **Passed Files** tab in the **Scan Result** page to view more detailed information about the passed files.
- **Failed Files** – The files that do not meet the defined scan policy. Select **View All** to go to the **Failed Files** tab in the **Scan Result** page to view more detailed information about the failed files.

If you want to view the trend report of the scan results, select the **Scan Result Trend Report** link and review it in the pop-up window. The passed files and failed files of the selected scan policy will be displayed in a histogram. You can specify a date range from **This Month**, **Last Month**, **Last 3 Months**, **Last 6 Months**, and **Last 12 Months** to view the passed files and failed files of the selected scan in the specified time range. The total number of passed files, failed files, unavailable files, and exceptional PDF files is the number of the files that need to be scanned in the specified scope.

Risk Report Overview

The Risk Report overview area provides a quick overview of the Risk Report results. The user can define a risk level for each check to represent the risk for files that do not obey this check.

A check is an XML file that defines the logic that Compliance Guardian Online uses to check files. Checks identify the purpose for the check (the type of check to run, such as a pattern of characters), the condition for the check (such as a social security number pattern), and the possible result of the check (true or false). Users can change the values in the checks to determine the check conditions, but the elements' specific format defined by Compliance Guardian Online in the checks must stay the same.

A test suite is a collection of checks. For each test suite, the risk of one file is calculated by the specified risk formula. The risk formula is a formula used for calculating a check's risk level. It provides the user with a method to increase risk at a level proportional to the risk type, while at the same time providing a method to grow risk at a specified factor, allowing for a real look at risk by occurrence.

- Raw risk of one file = (the first check's raw risk level calculated by the raw risk formula in the test suite) + (the second check's raw risk level calculated by the raw risk formula in the test suite) + … + (the last check's raw risk level calculated by the raw risk formula in the test suite)
- Stepped risk of one file = (the first check's stepped risk level calculated by the stepped risk formula in the test suite) + (the second check's stepped risk level calculated by the stepped risk formula in the test suite) + … + (the last check's stepped risk level calculated by the stepped risk formula in the test suite)
- Weighted risk of one file = (the first check's weighted risk level calculated by the weighted risk formula in the test suite) + (the second check's weighted risk level calculated by the weighted risk formula in the test suite) + … + (the last check's weighted risk level calculated by the weighted risk formula in the test suite)

All the files analyzed by the scan engine will be grouped into the following three types according to their risk levels:

- **High Priority**
- **Medium Priority**
- **Low Priority**

***Note:** For more information on high, medium, and low priority files, refer to the Risk Report section. The Risk Report displays all three types of files.

Select **View All Risk Report** to go to the **Risk Report** page to view more detailed information about the grouped files.

Violation Report Overview

The Violation Report overview area displays the violation files of each check and the percentage of those violation files. When there are more than 10 checks used, the scan results of the top 9 checks will be displayed in different colors. From the tenth check, all the results of the checks are displayed as **Others** in the pie chart. The Violation Type, Number of Violations, Number of Files, and Violation Percentage of those 10 areas will be displayed on the right pane.

If you hover over a sector in the pie chart, you can also view the Violation Type, Number of Violations, Number of Files, and Violation Percentage of the specified check. If you select a sector in the pie chart, you can view all the violation files and their locations in the pop-up window.

To export the detailed information to a CSV file for further use, select the **Export to Datasheet** link on the top-right corner of the pop-up window, and then enter a request name in the **Export to** window. Then select **OK** to export the file.

To view the trend report of the violation files, select the **Violation Report Trend Report** link and review it in the pop-up window. All the test suites of all the scan policies that have been involved in the scan jobs will be loaded and displayed in the **Test Suite Filter** drop-down menu. Select the checks containing the violation files you want to view from the **Test Suite Filter** drop-down menu, and then select **OK** to confirm the selection. After selecting **OK**, the violation files of the selected checks will be displayed in the **Violation Trend Report** window in lines of different colors and different formats. To view the violation files of the selected checks in a specified time range, choose from **This Month**, **Last Month**, **Last 3 Months**, **Last 6 Months**, or **Last 12 Months**.

To view more detailed information about the grouped files, select **View All Violation Report** to go to the **Violation Report** page.

Other Reports Overview

The Other Report overview area displays the other reports to view specific types of scanned results:

- **Data Table Report** – If the files analyzed by Compliance Guardian Online contain one or several tables, the corresponding files will be displayed in the Data Table Report. Those files must be reviewed manually to confirm whether it is accessible and compliant.
- **File Errors Report** – If the files specified for the compliance scanning failed to be scanned (for example, Compliance Guardian Online does not have enough permissions to access the specified files, or the files themselves are corrupted), those specified files will be considered as unavailable and will be recorded in the File Errors Report.

  If the scanned files cannot be analyzed by Compliance Guardian Online (due to an invalid file type, for example), they will also be recorded in the File Errors Report.

  ***Note**: The total number of passed files, failed files, unavailable files, and exceptional PDF files is the number of the files that need to be scanned in the specified scope.

- **File Type Report** – Groups the files analyzed by the scan engine according to their file type and display the scan results according to the grouped file types.
- **PDF Exception Report** – For the PDF files (generated using the Adobe Acrobat software), if Compliance Guardian Online finds out that those PDF files include unstructured textual content during the analyzing process, the corresponding PDF files will be recorded in the PDF Exception Report.

  ***Note:** Unstructured textual content is content that cannot be recognized by the scan engine. For example, if someone created a PDF from an image file instead of a MS Word file, the scan engine may not be able to scan and recognize any of the text in the PDF file. Therefore, that PDF file would show up in the PDF Exception Report.

- **Link Validation Report** – Groups the files that contain links and bookmarks that have been tested. The report is used to view the validity of the file's links or bookmarks.
- **Page Title Report** – The report is used to check the uniqueness of the webpage title (check the **<title>** node in the source code of the file). The files that do not have unique titles will be displayed in this report.

Types of Compliance Reports

You can access each of the following compliance report types. For more information about each of these reports, refer to the following sections:

- Scan Result Report
- Risk Report
- Data Table Report
- File Errors Report
- File Type Report
- PDF Exception Report
- Violation Report
- Link Validation Report
- Page Title Report
- Human Auditor
- Export Requests
- Export All Requests to HTML

The following actions can be performed at the lower right-hand corner of any report page:

- To change the number of the report result items displayed per page, select the desired number from **10** (default value), **15**, **20**, **30** in the **Show rows** drop-down menu.
- To go to the specified page, enter the page number in the **Page … of** text box and press **Enter** on your keyboard.
- To go to the next page, select the **>** button; to return to the previous page, select the **<** button.

Scan Result Report

To view details on all the files that are analyzed by the scan engine, select **Scan Result** on the navigation bar to open the **Scan Result** page and review the **Passed Files** Tab and **Failed Files** Tab.

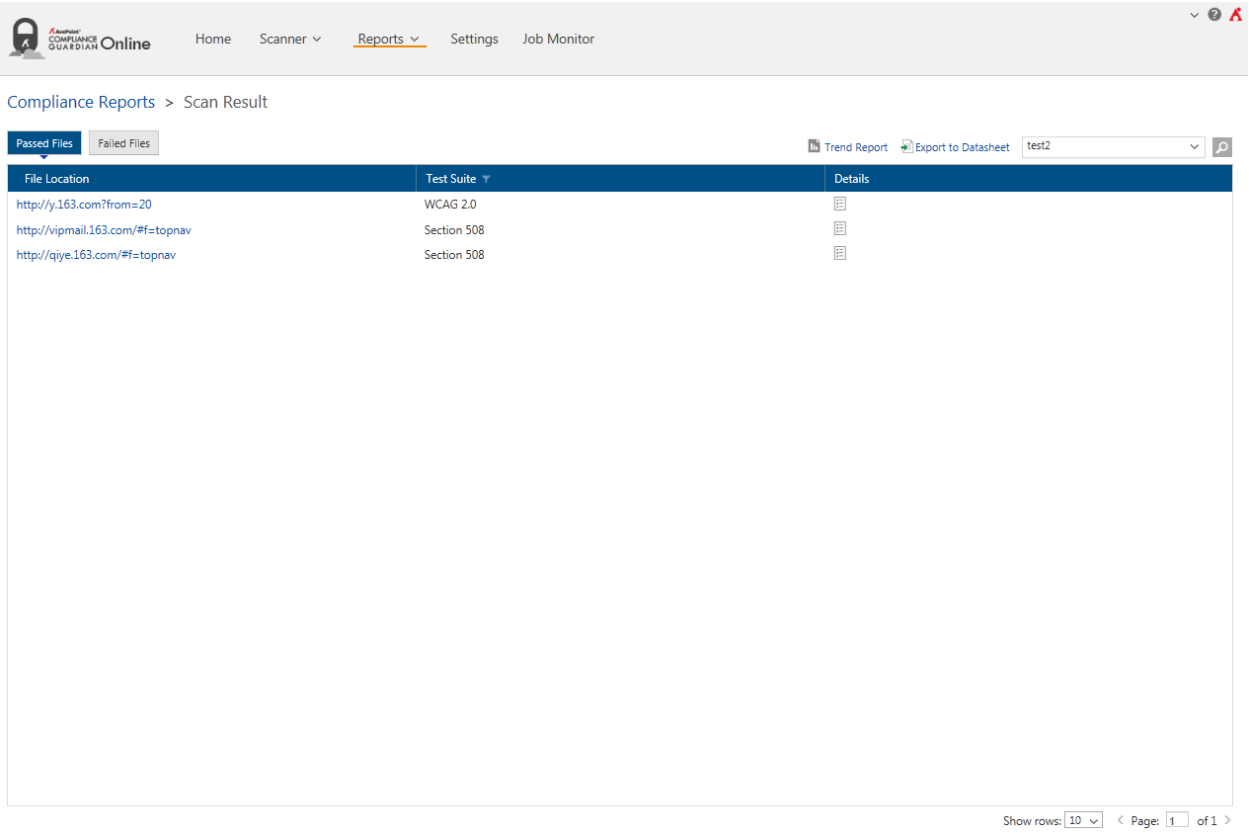

Figure 4: Scan Result report page.

To view a trend report as described in the Compliance Report Home Page section, select the **Scan Result Trend Report** link at the top of this page.

To export the scan results, complete the following steps:

1. Select the **Export to Datasheet** link on the top-right corner of this page.
2. Enter a request name in the **Export to** window.
3. Select **OK**. The request will start to run. You can go to the **Export Requests** interface to view the running process of the request.
4. After the request finishes running, select one request and download the compressed report files to a specified location.
5. Export the report to a CSV file to view all the items.

Passed Files Tab

When a scanned file obeys all the checks in the specified test suite (meaning there is no failed item for this file), its status will be considered as passed, and the file is a passed file. The **Passed Files** tab of the Scan Result page displays the following information:

- **File Location** – The full URL of the passed file. Selecting the URL in this column will redirect you to the specified file.
- **Test Suite** – The name of the test suite used for scanning this file.
    - After selecting the filter button ( ) in this column, selecting the desired test suites in the drop-down menu, and selecting **OK**, only the passed files of the selected test suites will be displayed in the table.
    - If you select **Select All** and select **OK**, the passed files of all the test suites will be displayed in the table.
    - Select **Cancel** if you want to cancel the selection.
- **Details** – Select the detail report button ( ) in the **Details** column to view the detailed information in the **View Detailed Report** window. Here you can view the following information:
    - **File Location** – The full URL of the specified file. Selecting the URL in this area will direct you to the specified file.
    - **Test Suite** – The name of the test suite used for scanning this file.
    - **Scan Time** – The time when this file was scanned.
    - **Status** – The status of this file regarding the whole test suite. In this case, because the scanned file obeys all the checks in the specified check collection (which means there is no failed item for this file), its status will be considered as passed. The file is therefore a passed file and the status will indicate **Passed**.
    - **Regulation** – The name of a specified regulation (check) included in the corresponding test suite. Select the regulation will be redirected to the webpage of the check policy URL.
    - **Description** – The description of this specified check.
    - **Status** – The status of this file regarding this specified check.
        - **Passed** – The file obeys the specified check.
        - **Failed** – The file disobeys the specified check.
        - **User Review Required** – The file needs the user to review it to decide its final status. For example, the file contains tables.
        - **Not Applicable** – The file does not contain the elements defined in the specified check.
        - **Not Tested** – The specified check is not checked for the specified file. When a check is included in the test suite of the scan policy used for

scanning this file, but the specified check is not enabled in the corresponding test suite, this status will be displayed.

        - **Warning** – The file contains violations.
    - **Change Status** – You can change the file's initial status by selecting the change status ( ) button in this column. For the detailed information, refer to Changing File's Initial Status.

You can search the files displayed by designating keywords. The keyword must be contained in a column value. At the top of the **Passed Files** viewing pane, select the search ( ) button, and then enter the keyword for the files you want to display in the text box.

Failed Files Tab

When a scanned file disobeys one or several checks in the specified test suite, its status will be considered as failed, and the file is a failed file. The **Failed Files** tab of the Scan Result page displays the following information:

- **File Location** – The full URL of the failed file. Selecting the URL in this column will redirect you to the specified file.
- **Test Suite** – The name of the test suite used for scanning this file. After selecting the filter button ( ) in this column, selecting the desired test suites in the drop-down menu and selecting **OK**, only the failed files of the selected test suites will be displayed in the table. If you select **All** and select **OK**, the failed files of all the test suites will be displayed in the table. If you select **None**, the selection status of the test suites will be cleared. Select **Cancel** if you want to cancel the selection.
- **Details** – Select the detail report button ( ) in the **Details** column to view the detailed information in the **View Detailed Report** window. Here you can view the following information:
    - **File Location** – The full URL of the specified file. Selecting the URL in this area will redirect you to the specified file.
    - **Test Suite** – The name of the test suite used for scanning this file.
    - **Scan Time** – The time when this file is scanned.
    - **Status** – The status of this file regarding the whole test suite. In this case, because the scanned file disobeys one or several checks in the specified test suite, the file is therefore a failed file and the status will indicate **Failed**.
    - **Regulation** – The name of a specified regulation (check) included in the corresponding test suite. Select the regulation will be redirected to the webpage of the check policy URL.
    - **Description** – The description of this specified check.
    - **Status** – The status of this file regarding this specified check.
        - **Passed** – The file obeys the specified check.

        - **Failed** – The file disobeys the specified check.
        - **User Review Required** – The file needs the user to review it to decide its final status. For example, the file contains tables.
        - **Not Applicable** – The file does not contain the elements defined in the specified check.
        - **Not Tested** – The specified check is not checked for the specified file. When a check is included in the test suite of the scan policy used for scanning this file, but the specified check is not enabled in the corresponding test suite, this status will be displayed.
        - **Warning** – The file contains violations.
    - **Change Status** – You can change the file's initial status by selecting the change status ( ) button in this column. For the detailed information, refer to Changing File's Initial Status.

      ***Note**: Only the user who has the **Human Auditor** permission can see this column.

- **Error Highlight Report** – Select the error highlight report button ( ) in the **Details** column to view the source of the specified file in the **Error Highlight Report** window. The contents that are not compliant will be highlighted in yellow so the users can locate those parts quickly and fix any compliance issues. In the pop-up window, you can also view the following information:
    - **File Location** – The full URL of the specified file. Selecting the URL in this area will redirect you to the specified file.
    - **Test Suite** – The name of the test suite used for scanning this file.
    - **Scan Time** – The time when this file is scanned.
    - **Status** – The status of this file regarding the whole test suite. In this case, because the scanned file disobeys one or several checks in the specified test suite, its status will be considered as failed. The file is therefore a failed file and the status will indicate **Failed**.

  If a file has been modified or deleted after it was scanned, after you view its Error Highlight Report, a message will appear in the Error Highlight Report to warn you that the result of this report is not correct.

You can search the files displayed by designating keywords. The keyword must be contained in a column value. At the top of the **Failed Files** viewing pane, select the search ( ) button, and then enter the keyword for the files you want to display.

Risk Report

To view the risk levels of each failed file, select **Risk Report** on the navigation bar to open the **Risk Report** page.

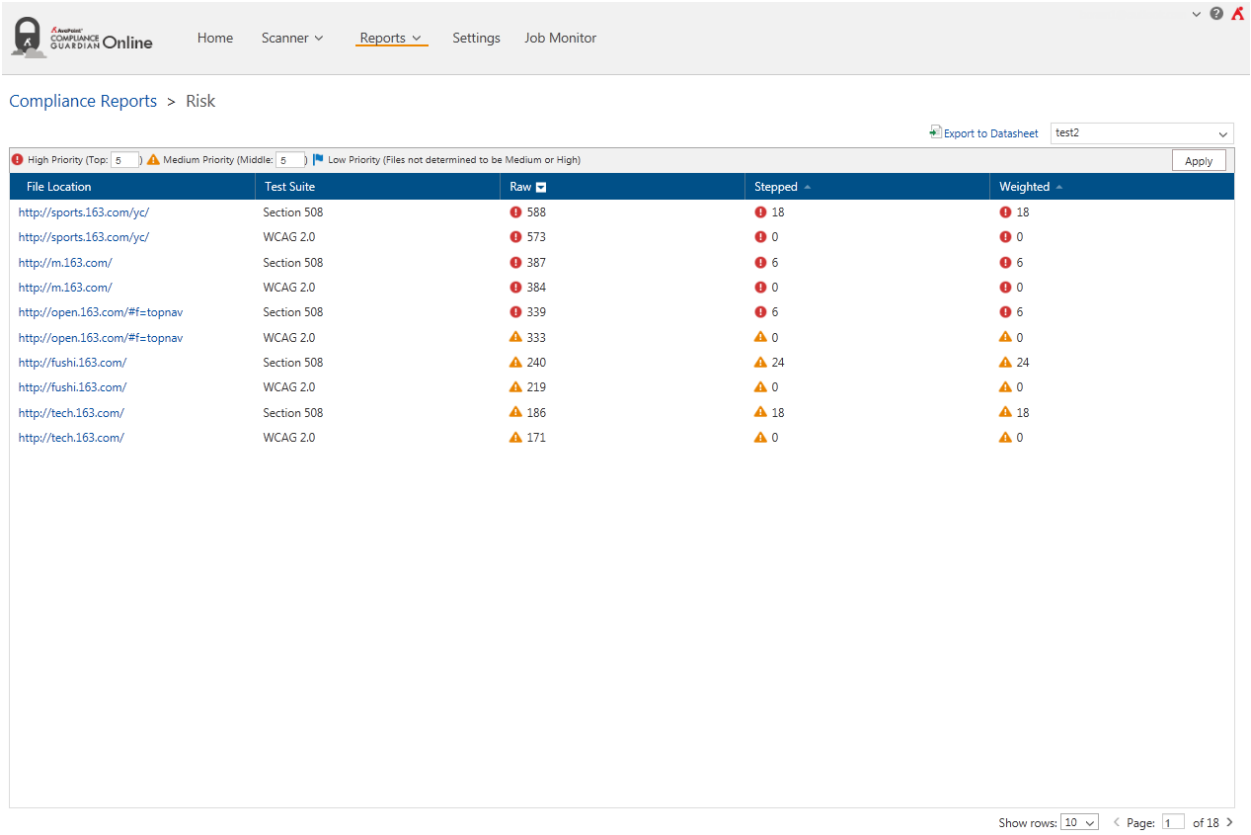
Compliance Guardian Online
Home
Scanner
Reports
Settings
Job Monitor
Compliance Reports > Risk
Export to Datasheet
test2
High Priority (Top: 5) Medium Priority (Middle: 5) Low Priority (Files not determined to be Medium or High)
Apply
File Location
Test Suite
Raw
Stepped
Weighted
http://sports.163.com/yc/ Section 508 588 18 18
http://sports.163.com/yc/ WCAG 2.0 573 0 0
http://m.163.com/ Section 508 387 6 6
http://m.163.com/ WCAG 2.0 384 0 0
http://open.163.com/#f=topnav Section 508 339 6 6
http://open.163.com/#f=topnav WCAG 2.0 333 0 0
http://fushi.163.com/ Section 508 240 24 24
http://fushi.163.com/ WCAG 2.0 219 0 0
http://tech.163.com/ Section 508 186 18 18
http://tech.163.com/ WCAG 2.0 171 0 0
Show rows: 10
Page: 1 of 18

Figure 5: Risk report page.

To define the number of the high priority files, medium priority files, and low priority files, enter the desired number in the corresponding **High Priority** and **Medium Priority** text boxes above the table. The rest of the files will be designated as **Low Priority** files. The files in the downloaded report will be grouped according to the specified numbers:

- Files with higher risk levels require more attention and usually need to be dealt with immediately.
- Files with lower risk levels are relatively less threatening to the community, and can be dealt with after you have fixed the compliance issues in the files of higher priority.

The three different kinds of risk priority files are marked with three different colors. The colors will be displayed accordingly for the files with the corresponding risk priority, designed for a direct and clear view of all the failed files.

The following information is displayed on this page:

- **File Location** – The full URL of the specified file. If you select the URL in this column, you will be redirected to the specified file.
- **Test Suite** – The test suite which is used by the corresponding file.
- **Raw** – The risk levels calculated by the **Raw** type risk formula are displayed in this column. The Raw type risk formula is **r1*n**.
- **Stepped** – The risk levels calculated by the **Stepped** type risk formula are displayed in this column. The Stepped type risk formula is **r1+r2*(n-1)**.
- **Weighted** – The risk levels calculated by the **Weighted** type risk formula are displayed in this column. The Weighted type risk formula is **r1+r2*r3*(n-1)**.

  Refer to the following information for the meaning of r1, r2 and r3:

  - **r1** – Item Initial Risk value, this is the value assigned on the initial occurrence of the compliance failure (related to the check being tested for) in the document or stream.

    Allowed Values for r1 are 1-10.

  - **r2** – Item Additional Risk Level factor (Step) that the risk level grows at for every additional failure at the check level (for the same type) found in the document or stream. This number is optional where the integer "-1" means ignore the value (allowing to use the third value). If the value is -1 then the factor will be 1.

    Allowed Values are -1 to 10.

  - **r3** – Item risk in relation to other checks. This Item is optional. If this number is missing then it is assumed that its value is "1".

    Allowed Values are 1-10.

    In addition, the r3 value allows us to define importance of an item in a check against other checks allowing us to look at a page with 100 images with missing alternative text quite differently than a page that has 100 social security numbers. In addition, if we considered alt text errors and SSN numbers as errors that should grow risk at the same value for every new occurrence we could then define importance at a higher level for a specified test suite. These two additional risk factors allow us to more accurately show risk against checks or test suites and based on importance of repetitive failure in a document.

To export the risk report results, complete the following steps:

1. Select the **Export to Datasheet** link on the top-right corner of this page.
2. Enter a request name in the **Export to** window.

3. Select **OK**. The detailed information displayed on this page will be exported to a CSV file for further use.

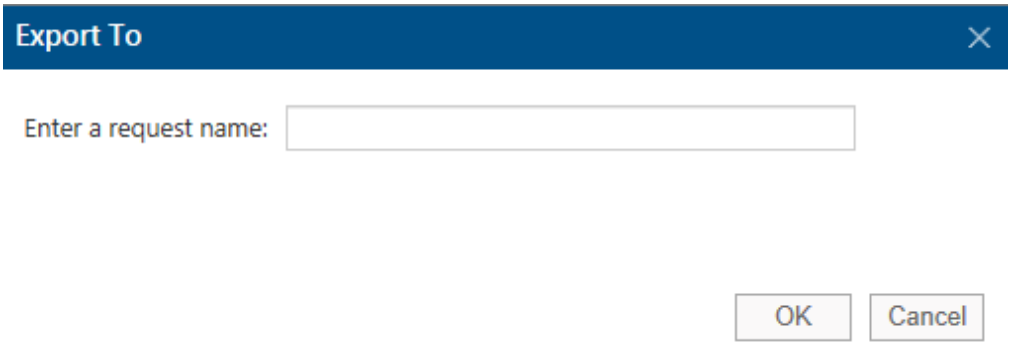

Figure 6: Export To window.

Data Table Report

Select **Data Table Report** on the navigation bar. You will be brought to the Data Table Report page. You can also directly select **Data Table Report** under the **Other Reports** field in the Compliance Report Page. The Data Table Report page provides a view of all the files that contain tables. Those files must be manually reviewed to check whether they are compliant and to verify their accessibilities.

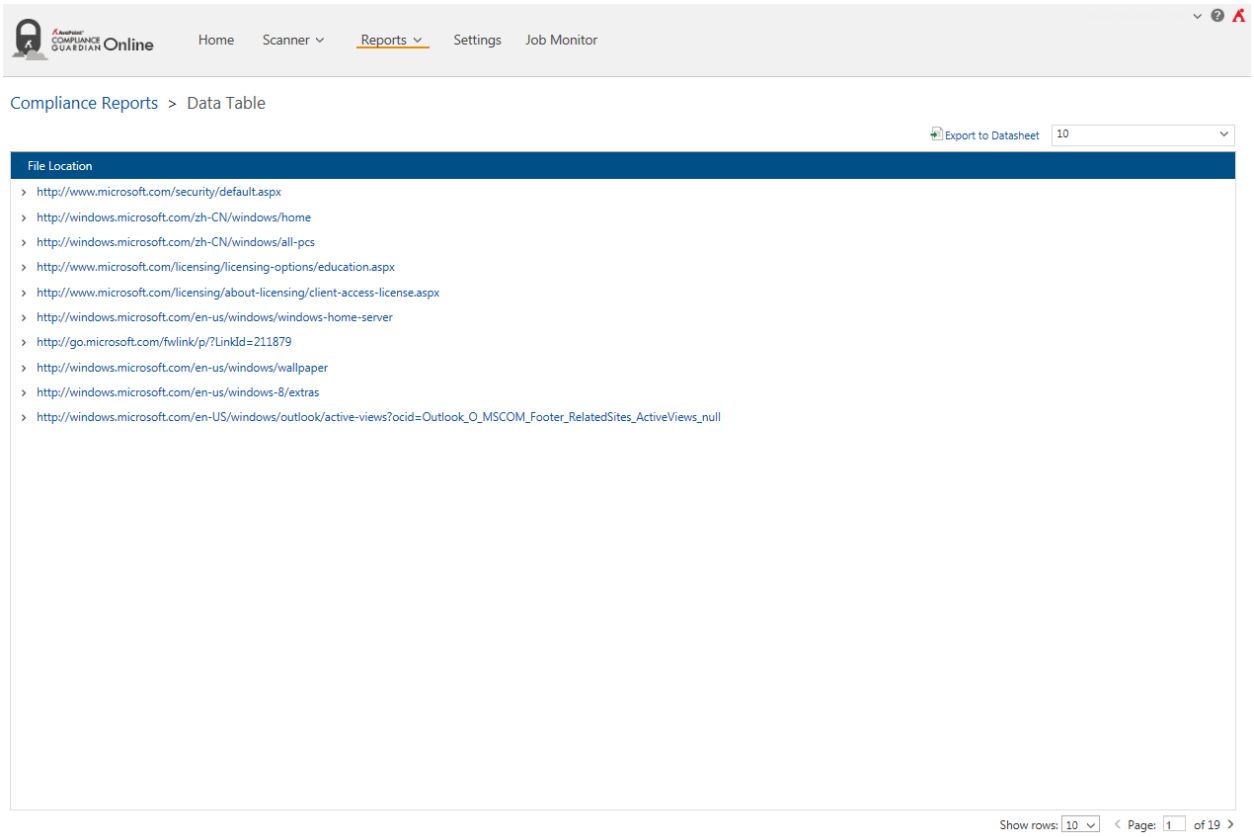

Figure 7: Data Table Report page.

The **File Location** table on this page displays full URLs of the specified files. Selecting a URL in this column will redirect you to the specified file. After selecting the right arrow (›) next to the file's URL, the detailed locations of the tables will be displayed in the expanded Details area. The format is: Line 100, Column 100.

Select the **Export to Datasheet** link on the top-right corner of this page, enter a request name in the Export to window, and then select **OK**. The detailed information displayed on this page will be exported to a CSV file for further use.

File Errors Report

Select File Errors Report on the navigation bar. You will be brought to the File Errors Report page. You can also directly select **File Errors Report** under the **Other Reports** field in the Compliance Report Home Page. You can view all the files that cannot be retrieved and downloaded on the **File Errors Report** page.

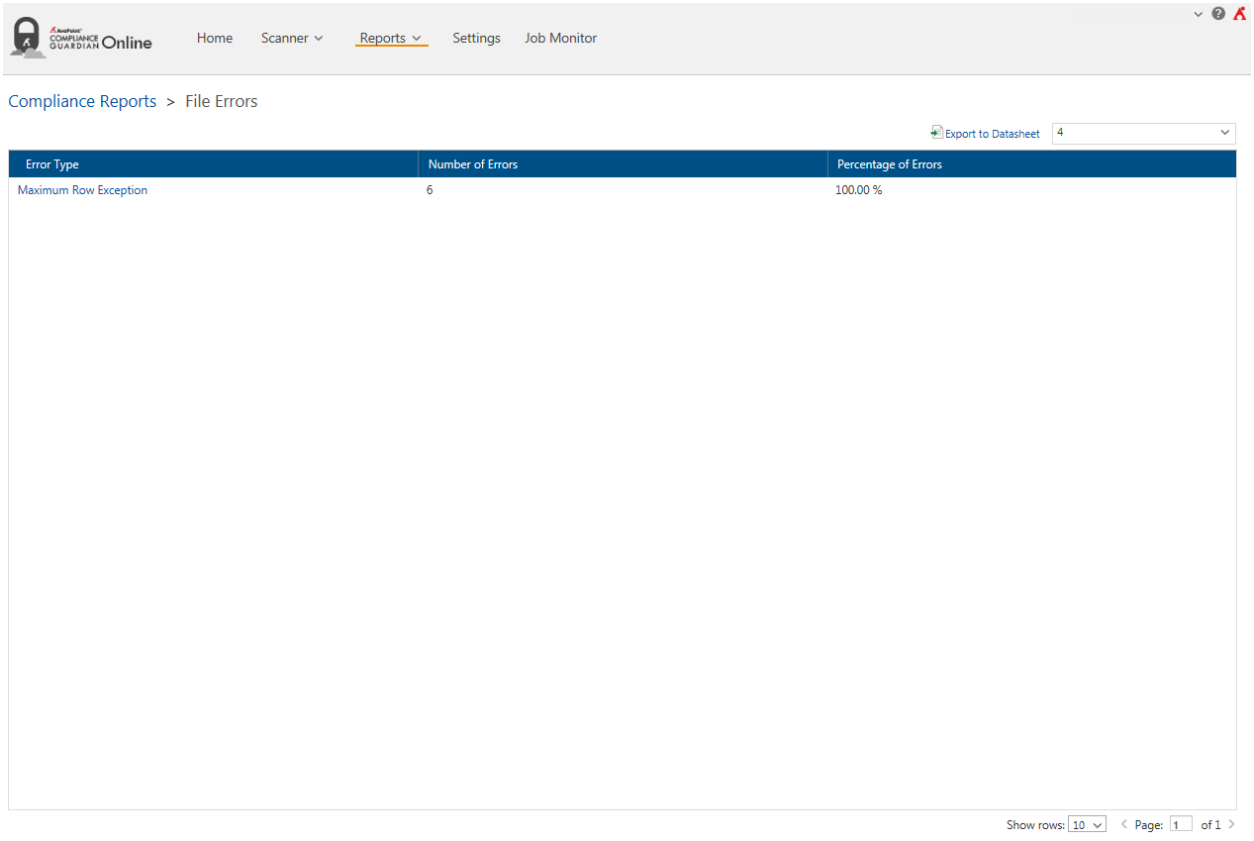

Figure 7: File Errors Report page.

The following information is displayed on this page:

- **Error Type** – Displays the type of the specified error. Selecting the displayed error, the **Error Details** interface appears and it displays the following information:

- **File Location** – The full URL of the specified file. Selecting the URL in this column will redirect you to the specified file.
- **Details** – The detailed error information of this specified type of error.

- **Number of Errors** – The number that the specified error occurs.
- **Percentage of Errors** – The percentage of this specified error in all the errors found. If you add the value in this column for each kind of error, you will get 100%.

Select the **Export to Datasheet** link on the top-right corner of this page, enter a request name in the **Export to** window, then select **OK** and the detailed information displayed on this page will be exported to a CSV file for further use.

File Type Report

Select **File Type Report** on the navigation bar. You will be brought to the **File Type Report** page. You can also directly select **File Type Report** under the **Other Reports** field in the Compliance Report Home Page. You can view all the scanned files' types and each file type's percentage on the **File Type Report** page.

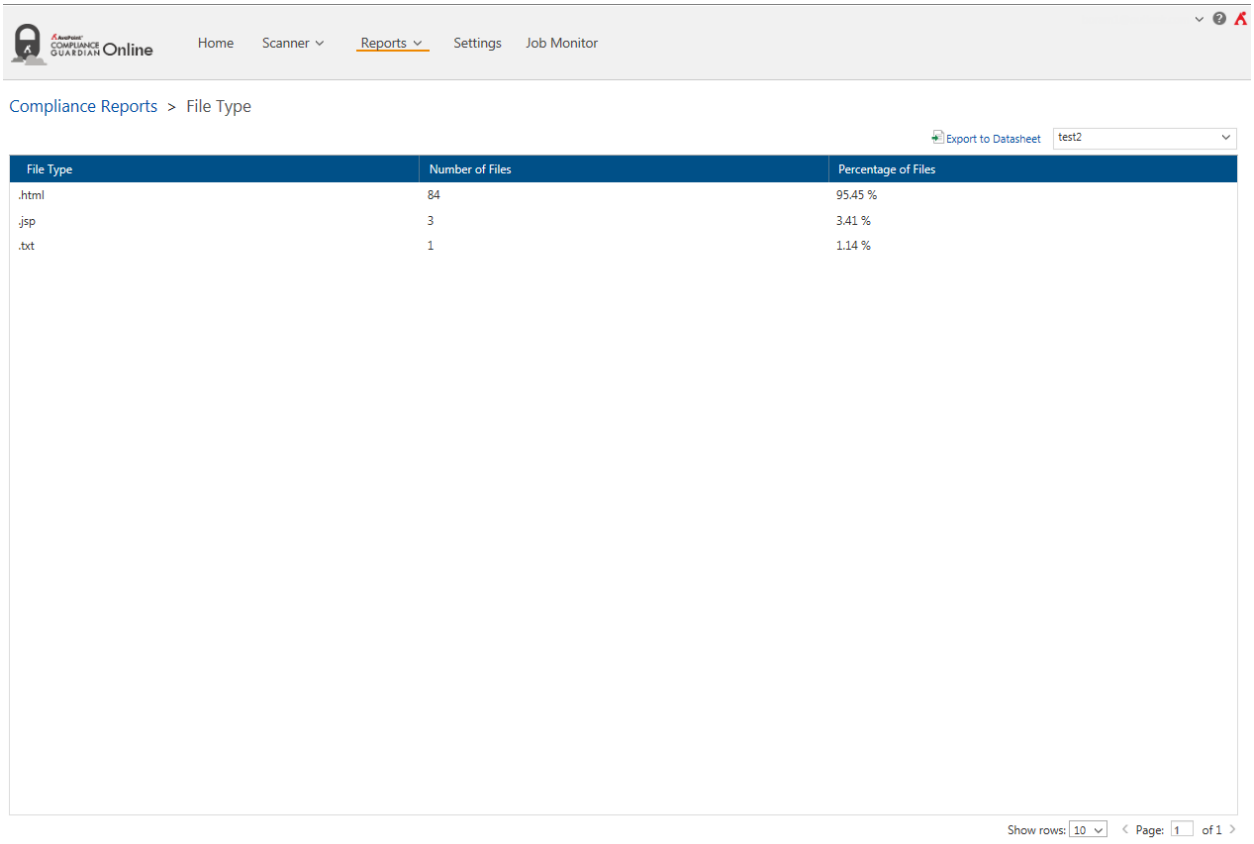

Figure 8: File Type Report page.

The following information is displayed on this page:

- **File Type** – One type of all the scanned files.

- **Number of Files** – The number of the scanned files that are of the specified file type.
- **Percentage of Files** – The percentage of the specified type of files in all the scanned files. If you add the value in this column for each file type, you will get 100%.

Select the **Export to Datasheet** link on the top-right corner of this page, enter a request name in the **Export to** window, then select **OK** and the detailed information displayed on this page will be exported to a CSV file for further use.

PDF Exception Report

Select **PDF Exception Report** on the navigation bar. You will be brought to the **PDF Exception Report** page. You can also directly select **PDF Exception Report** under the **Other Reports** field in the Compliance Report Home Page. The **PDF Exception Report** page provides a view of all the PDF files (generated using the Adobe Acrobat software) that contain unstructured textual content.

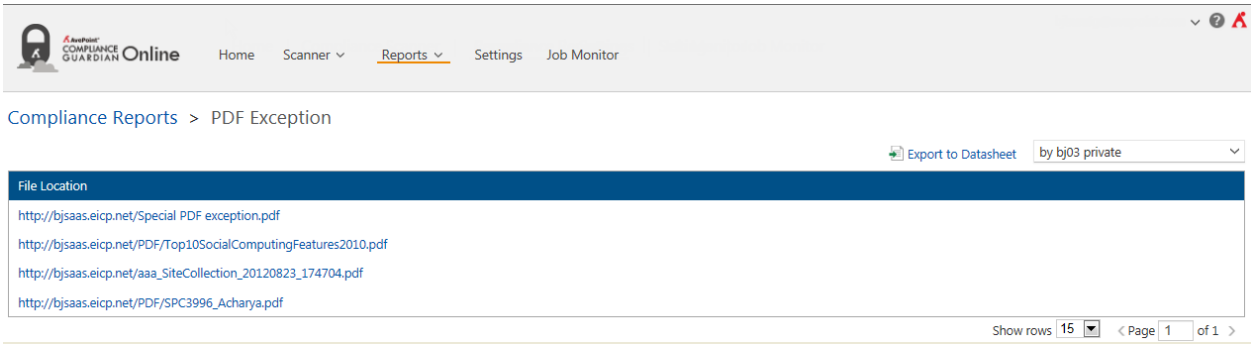

Figure 9: PDF Exception Report page.

The **File Location** table on this page displays full URLs of the specified files. Selecting a URL in this column will redirect you to the specified file.

Select the **Export to Datasheet** link on the top-right corner of this page, enter a request name in the **Export to** window, then select **OK** and the detailed information displayed on this page will be exported to a CSV file for further use.

Violation Report

Select **Violation** on the navigation bar. You will be brought to the **Violation Report** page. You can also directly select **View All Violation Report** under the **Violation Report** field on the Compliance Report Home Page. The Violation Report page displays all the classified violation files of each check.

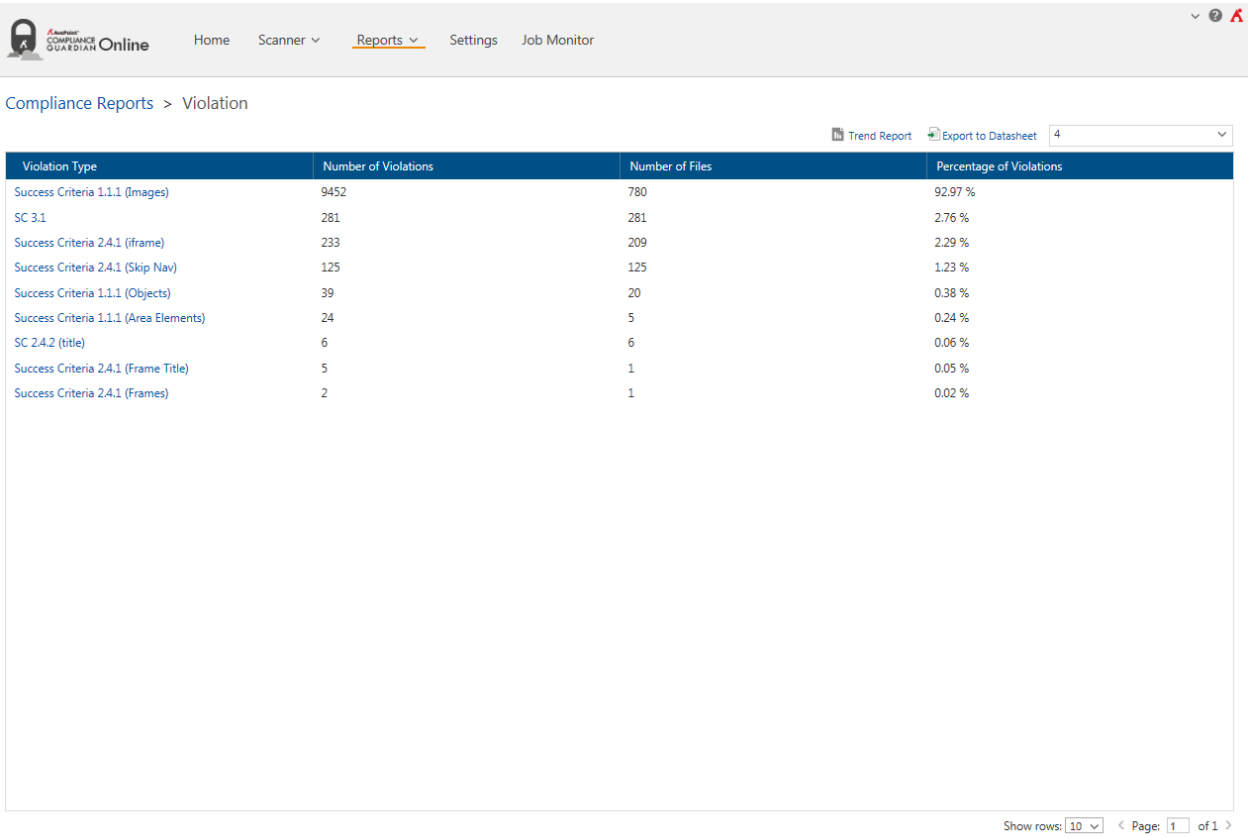
Online
Home
Scanner
Reports
Settings
Job Monitor
Compliance Reports > Violation
Trend Report
Export to Datasheet
4
Violation Type
Number of Violations
Number of Files
Percentage of Violations
Success Criteria 1.1.1 (Images) 9452 780 92.97 %
SC 3.1 281 281 2.76 %
Success Criteria 2.4.1 (iframe) 233 209 2.29 %
Success Criteria 2.4.1 (Skip Nav) 125 125 1.23 %
Success Criteria 1.1.1 (Objects) 39 20 0.38 %
Success Criteria 1.1.1 (Area Elements) 24 5 0.24 %
SC 2.4.2 (title) 6 6 0.06 %
Success Criteria 2.4.1 (Frame Title) 5 1 0.05 %
Success Criteria 2.4.1 (Frames) 2 1 0.02 %
Show rows: 10
Page: 1 of 1

Figure 10: Violation Report page.

The following information is displayed on this page:

- **Violation Type** – The name of one specified check. After selecting the link in this column, the following information will be displayed in a pop-up window:
    - **Check Name and Description** – At the top-left corner of the pop-up window, it displays the name of the specified check and the brief introduction to this check.
    - **File Location** – The full URL of the specified violation file of this check. Selecting the URL in this column will redirect you to the specified file.
- **Number of Violations** – The number of violations counted for this check.
- **Number of Files** – The number of the violation files of the specified check.

- **Percentage of Violations** – The percentage of the specified check's violation files of all the violation files. If you add the value in this column for each check, you will get 100%.

To view the Trend Report as described in the Compliance Report Home Page section, select the **Violation Trend Report** link in the top-left corner of this page.

Select the **Export to Datasheet** link on the top-right corner of this page, enter a request name in the **Export to** window, then select **OK** and the detailed information displayed on this page will be exported to a CSV file for further use.

Link Validation Report

Select **Link Validation Report** on the navigation bar. You will be brought to the **Link Validation Report** page. You can also directly select **Link Validation Report** under the **Other Reports** field in the Compliance Report Home Page. The **Link Validation Report** page provides a view all the tested files that contain links.

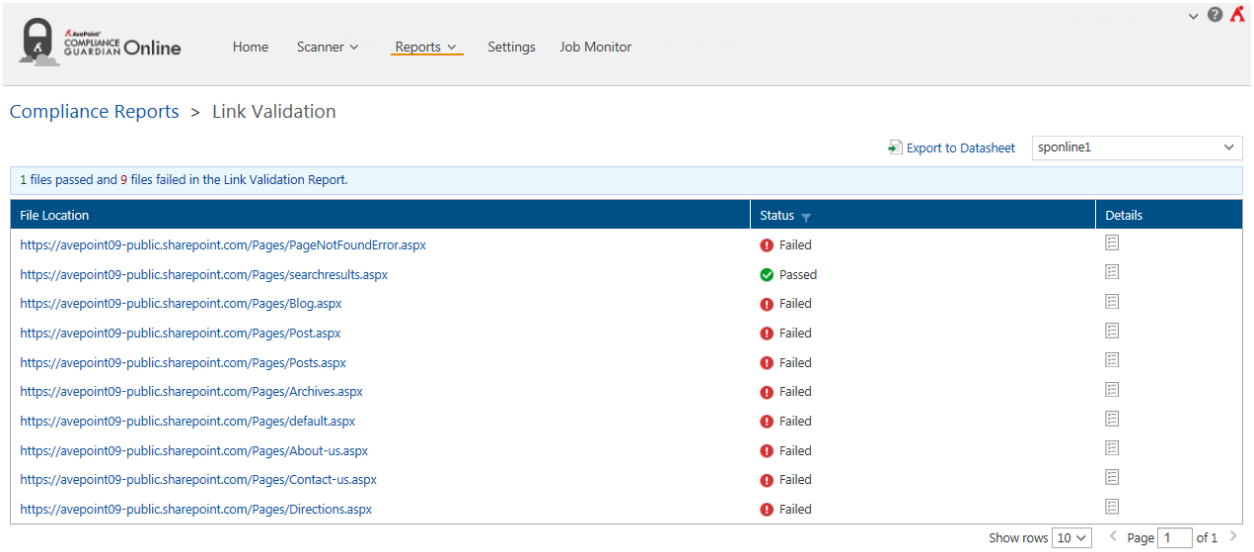

Figure 11: Link Validation Report page.

The following information is displayed on this page:

- **File Location** – The full URL of the specified file. Selecting the URL in this column will redirect you to the specified file.
- **Status** – The status of this file regarding this specified regulation (check).
  - **Passed** – The file obeys the specified check.
  - **Failed** – The file disobeys the specified check.

- **Details** – Select the detail report button ( ) in the **Details** column to view details in the **View Detailed Report** window. Here you can view the following information:
    - **File Location** – The corresponding file path. Selecting the URL in this area will direct you to the specified file.
    - **Link Details Field** – This field can list four conditions: 4XX Client Error, 5XX Server Error, Unknown Errors, and List of Redirects.
        - **4XX Client Error** – If there are some links in the file with a 4XX status code, they will be grouped in this field. This field also displays the link's error type, the link location in the file, and the error description.
        - **5XX Server Error** – If there are some links in the file with a 5XX status code, they will be grouped in this field. This field also displays the link's error type, the link location in the file, and the error description.
        - **Unknown Errors** – If there are some links with status codes that cannot be obtained due to some unknown exceptions, the links will be listed in this field. The location of the link and the corresponding error message will also display in this field.
        - **List of Redirects** – This field lists all the links that redirect to other URLs. The locations of these links will also display in this field.

        ***Note:** If the file does not contain the condition 4XX Client Error, 5XX Server Error, Unknown Errors, or List of Redirects, the corresponding field will not be displayed in the **View Detailed Report** window.
    - **Anchors** – This field displays all the anchors that are found in the file, as well as the invalid anchors.

        ***Note:** If there are no anchors found in the file, this field will not be displayed in the **View Detailed Report** window.

Select the **Export to Datasheet** link on the top-right corner of this page, enter a request name in the **Export to** window, and then select **OK**. The detailed information displayed on this page will be exported to a CSV file for further use.

Page Title Report

Select **Page Title** on the navigation bar. You will be brought to the **Page Title Report** page. You can also directly select **Page Title Report** under the **Other Reports** field in the Compliance Report Home Page. You can see all the files that do not have unique titles in the Page Title Report page.

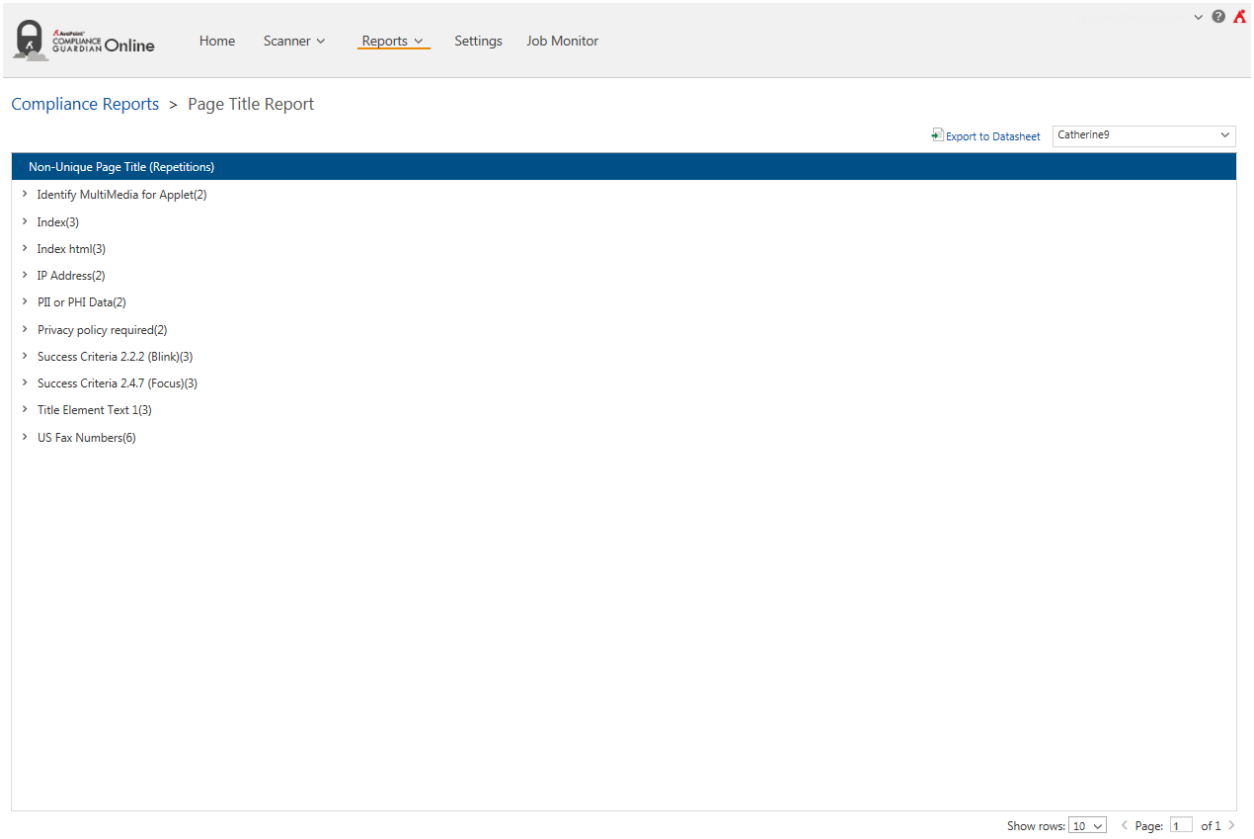

Figure 12: Page Title Report page.

The **Non-unique Page Title (Repetitions)** table displays the repetitive titles grouped by domain. If you select the triangle button (>) before a title, the files with this title that are in the same domain will be displayed. Select the file to open it.

Select the **Export to Datasheet** link on the top-right corner of this page, enter a request name in the **Export to** window, then select **OK** and the detailed information displayed on this page will be exported to a CSV file for further use.

Export Requests

Select **Export Requests** on the navigation bar. You will be brought to the **Export Requests** page. You can view all your own downloading requests of the report files on the Export Requests page.

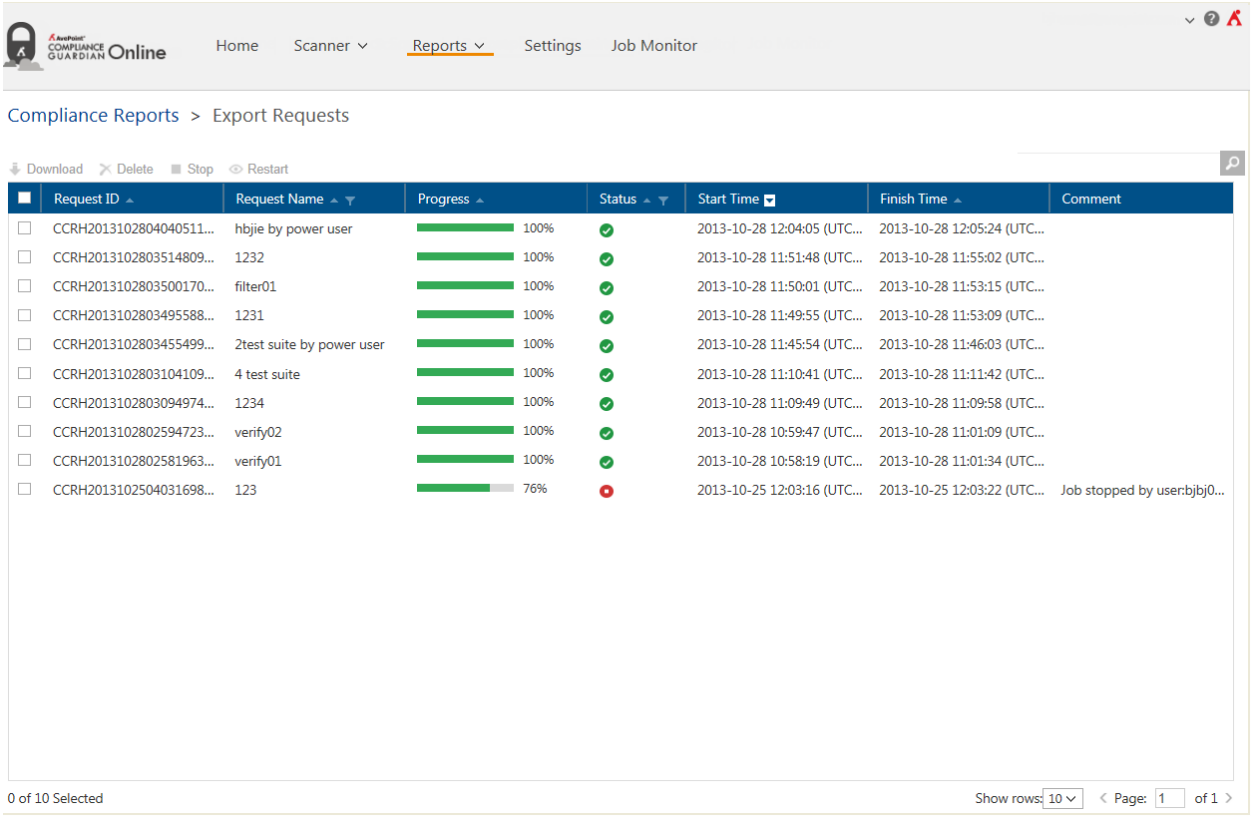

Figure 13: Export Requests page.

The following information appears on this page:

- **Request ID** – The ID of your report downloading request.
- **Request Name** – The name of your report downloading request.
- **Progress** – The progress of the downloading process.
- **Status** – The status of your report downloading request.
- **Start Time** – The start time of the report downloading process.
- **Finish Time** – The finish time of the report downloading process.
- **Comment** – The comment of the request.

The following actions can be performed in the **Export Requests** page:

- **Download** – Select one request, and then select this button to download the compressed report files to your specified location.

- **Delete** – Select one or several requests, and then select this button to delete the requests from the requests' list.
- **Stop** – Select one request, and then select this button to stop the report generating process.
- **Restart** – Select one request, and then select this button to restart the report generating process.

Human Auditor

Human Auditor allows you to change the initial status of a file, while tracking and auditing these changes. Select **Human Auditor** on the navigation bar.

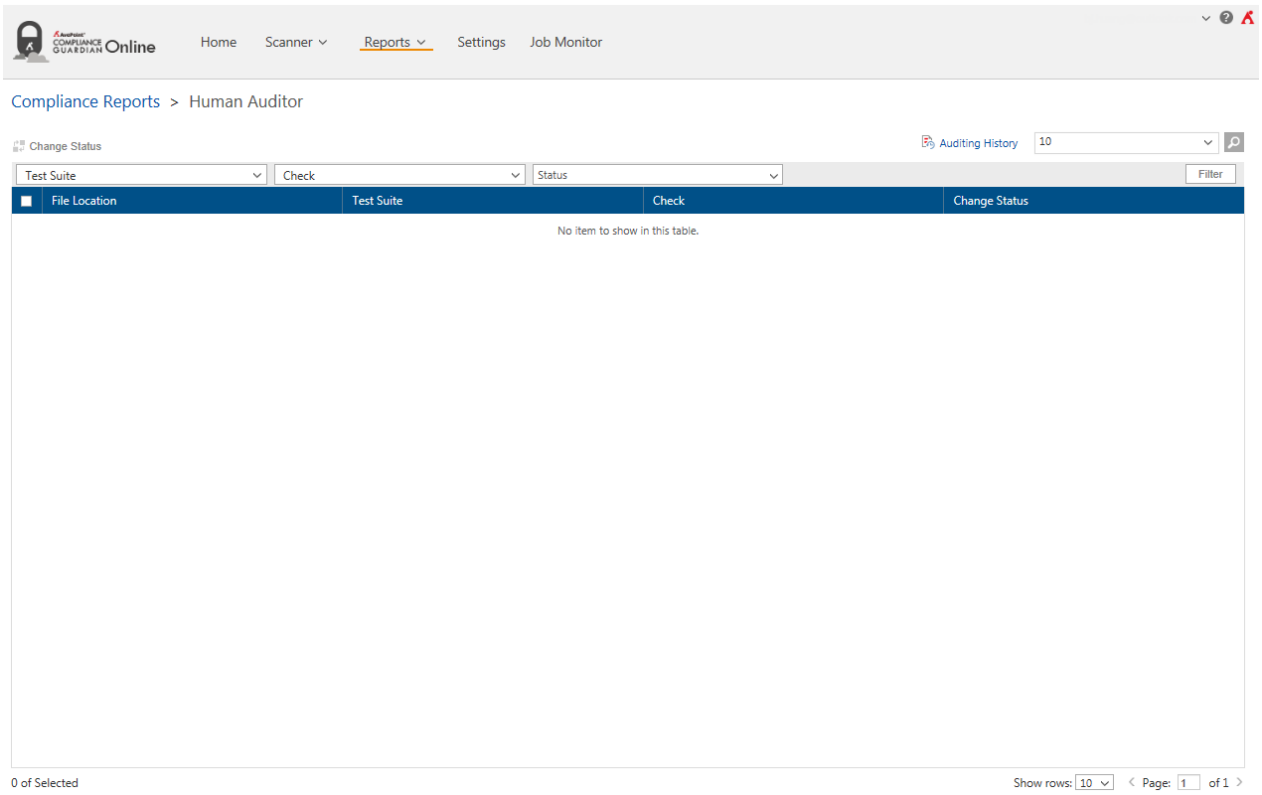

Figure 14: Human Auditor interface.

Select the test suites in the **Test Suite** drop-down list, you can also search the specified test suites by entering the keyword in the search field of the drop-down list. Select checks in the **Check** drop-down list, you can also search the specified checks by entering the keyword in the search field of the drop-down list. Then, select the check status in the **Status** drop-down list. Select **Filter**, the files that are scanned according to the selected checks, and whose status is the selected status are displayed in the table.

You can search the files displayed by designating the keyword or file URL. The keyword must be contained in a column value. Above the files viewing pane, enter keywords in the text box that appears after you select on the search ( ) button to search for the files you want to display.

Changing File's Initial Status

To change a file's initial status, complete the following steps:

1. Select the change status ( ) button in the **Change Status** column to change a file's initial scan status. You can also select the checkbox before a file, and then select **Change Status** above the table. The **Change Status** window appears.
2. Configure the following settings:
    - Select a status in the **Change status to** drop-down list.
    - Add an optional comment for this change.
    - Select the **Ignore this file until the file or test suites change** checkbox. The file will not be scanned until the test suites are changed, or until the file is changed.

Select **OK** in the **Change Status** window to save the changes, or select **Cancel** to return to the **Human Auditor** interface without saving any changes.

Auditing History

Select **Auditing History** on the upper-right corner of the Human Auditor interface to view the history of status changes. In the **Auditing History** interface, you can view the file's updated Time (the time of changing the file's initial status), the User who updated the file's status, the File Location, the related Check, the related Test Suite, the Initial Status, the Updated Status, the Comment. You also have the option to make the **Whether to Ignore this File Until the File or Test Suites Change** column display in the Auditing History interface

You can filter the files displayed by the keyword you designate. The keyword must be contained in a column value. At the top of the viewing pane, enter the keyword for the files you want to display.

Select the **Export to Datasheet** link on the top-right corner of this interface, enter a request name in the **Export to** window, and then select **OK**. The detailed information displayed on this interface will be exported to a CSV file for further use.

Export All Requests to HTML

Select **Export All Requests to HTML** on the navigation bar. You will be brought to the **Export All Requests to HTML** page. You can export the request to an HTML file which is used to view the Compliance reports.

To get started with the function, select a scan from the **Scan Filter** drop-down list at the top-right corner. Refer to the following section for exporting reports on websites and on SharePoint Online sites.

Configuring Export Report Settings for Reports on Websites

If you have selected a scan that is used to scan the website content, all of the test suites used in the selected scan will be displayed. Select the expand button (⊞) before a test suite to expand a test suite and display all of the checks.

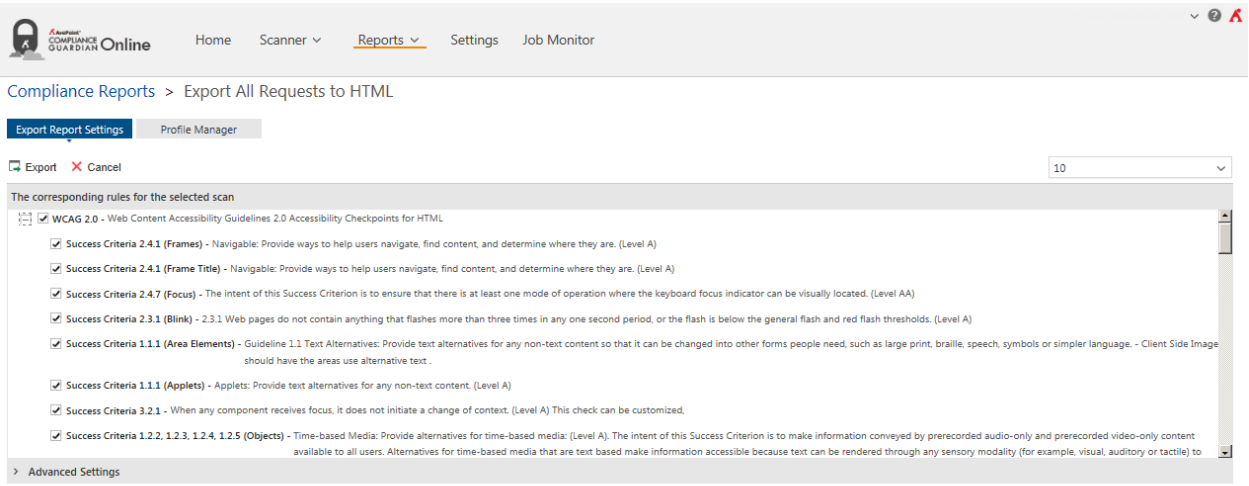
Online
Home
Scanner
Reports
Settings
Job Monitor
Compliance Reports > Export All Requests to HTML
Export Report Settings
Profile Manager
Export
Cancel
10
The corresponding rules for the selected scan
WCAG 2.0 - Web Content Accessibility Guidelines 2.0 Accessibility Checkpoints for HTML
Success Criteria 2.4.1 (Frames) - Navigable: Provide ways to help users navigate, find content, and determine where they are. (Level A)
Success Criteria 2.4.1 (Frame Title) - Navigable: Provide ways to help users navigate, find content, and determine where they are. (Level A)
Success Criteria 2.4.7 (Focus) - The intent of this Success Criterion is to ensure that there is at least one mode of operation where the keyboard focus indicator can be visually located. (Level AA)
Success Criteria 2.3.1 (Blink) - 2.3.1 Web pages do not contain anything that flashes more than three times in any one second period, or the flash is below the general flash and red flash thresholds. (Level A)
Success Criteria 1.1.1 (Area Elements) - Guideline 1.1 Text Alternatives: Provide text alternatives for any non-text content so that it can be changed into other forms people need, such as large print, braille, speech, symbols or simpler language. - Client Side Image should have the areas use alternative text .
Success Criteria 1.1.1 (Applets) - Applets: Provide text alternatives for any non-text content. (Level A)
Success Criteria 3.2.1 - When any component receives focus, it does not initiate a change of context. (Level A) This check can be customized.
Success Criteria 1.2.2, 1.2.3, 1.2.4, 1.2.5 (Objects) - Time-based Media: Provide alternatives for time-based media: (Level A). The intent of this Success Criterion is to make information conveyed by prerecorded audio-only and prerecorded video-only content available to all users. Alternatives for time-based media that are text based make information accessible because text can be rendered through any sensory modality (for example, visual, auditory or tactile) to
Advanced Settings

Figure 15: Export All Requests to HTML interface (exporting reports on websites).

Select the test suites or checks. The related report will be exported an HTML file.

You can also configure the advanced settings for the report. Select **Advanced Settings**, and then configure the following settings:

- **File Types Showed in Reports** – Select the file types. The report of the selected file types will be included in the exported report. You can customize the file type by selecting the **Specify file types** checkbox and entering the customized file types. Use the semicolon (**;**) as the separator.
- **Customize Exported Report** – Customize the header image, alt text for the header image, footer image, and alt text for the footer image for the exported report. Select **Browse** to select a header or footer image, or select **Reset** to clear your selected image and return to displaying the default image, and then reselect another image.

Configuring Export Settings for Reports on SharePoint Online Sites

If you have selected a scan that is used to scan the SharePoint Online sites, the related SharePoint Online sites tree is displayed under the **Scan Files Location** pane. The scan's related test suites are displayed in the right pane.

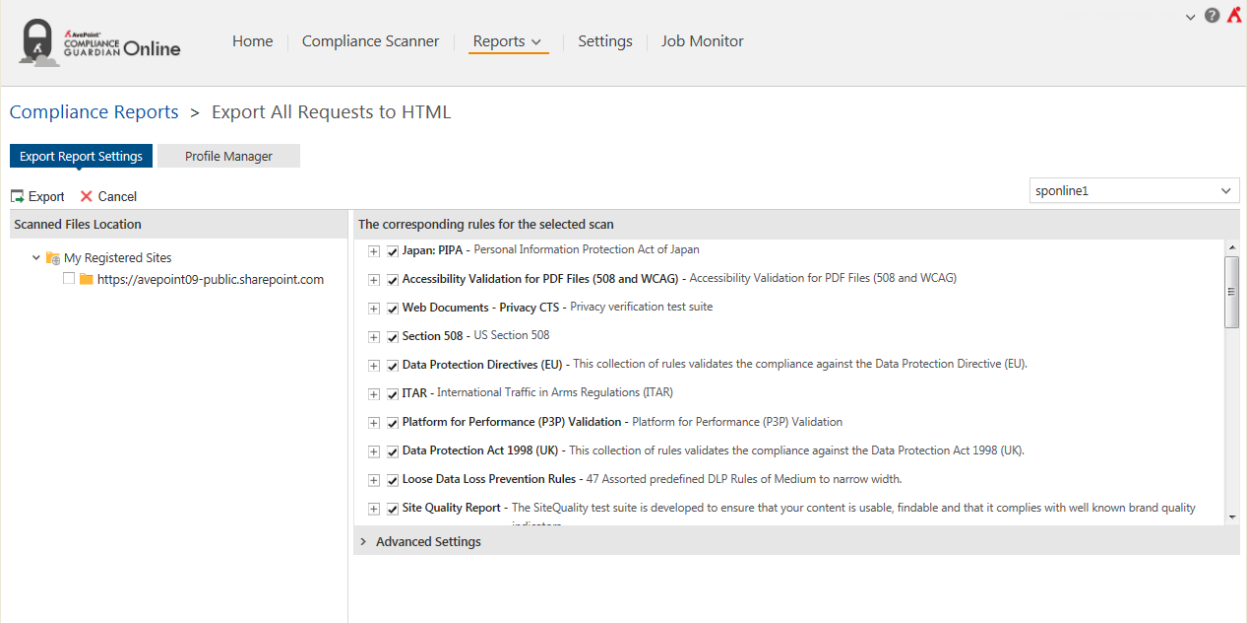
Online
Home
Compliance Scanner
Reports
Settings
Job Monitor
Compliance Reports > Export All Requests to HTML
Export Report Settings
Profile Manager
Export
Cancel
sponline1
Scanned Files Location
My Registered Sites
https://avepoint09-public.sharepoint.com
The corresponding rules for the selected scan
Japan: PIPA - Personal Information Protection Act of Japan
Accessibility Validation for PDF Files (508 and WCAG) - Accessibility Validation for PDF Files (508 and WCAG)
Web Documents - Privacy CTS - Privacy verification test suite
Section 508 - US Section 508
Data Protection Directives (EU) - This collection of rules validates the compliance against the Data Protection Directive (EU).
ITAR - International Traffic in Arms Regulations (ITAR)
Platform for Performance (P3P) Validation - Platform for Performance (P3P) Validation
Data Protection Act 1998 (UK) - This collection of rules validates the compliance against the Data Protection Act 1998 (UK).
Loose Data Loss Prevention Rules - 47 Assorted predefined DLP Rules of Medium to narrow width.
Site Quality Report - The SiteQuality test suite is developed to ensure that your content is usable, findable and that it complies with well known brand quality
Advanced Settings

Figure 16: Export All Requests to HTML interface (exporting reports on SharePoint Online sites).

Select the node in the SharePoint Online sites tree in the left pane, the related report will be included in the exported HTML file.

Select the expand (⊞) button before a test suite to expand the test suite for displaying all of the checks in the test suite. Select the test suites or checks. The related report will be exported an HTML file.

You can also configure the advanced settings by selecting the right arrow (›) before **Advanced Settings**:

- **File Types Showed in Reports** – Select one of the following options:
  - **All types** – All of the file types will be included in the report.
  - **Specify file types** – Select this radio button to define specified file types. Select the specified file types by selecting the checkboxes before the types. You can customize the file type **file types** by selecting the checkbox before the **Customized Type** field and entering the customized file types in this field. Use a semicolon (**;**) as a separator.
- **Specify the users. The files that are created or modified by these users will be displayed in the report** – Select one of the following options:
  - **Anyone** – The files that are created or modified by anyone will be displayed in the report.
  - **Specify users** – Select this radio button to define specified users. The filter condition field appears under this radio button. Select **Add a Criterion** to add a criterion. Then select a rule: **Created By** or **Modified By**. Select the condition (**Contains**, **Does Not Contain**, **Equals**, **Does Not Equal**, **Matches**, **Does Not Match**), and then enter a value. Select the checkbox before a criterion and then select **Remove** to delete the criterion.

*__Note:__ If the condition **Equals** or **Matches** is selected, you must add the claim type in front of the value.

Depending on the filters you enter, you can change the logical relationships between the filter rules. There are currently two logical relationships: **And** and **Or**. The logic is set to **And**. To change the logical relationship, select the logical relationship link. The **And** logical relationship means that the content which meets all of the rules will be filtered and included in the result. The **Or** logic means that the content which meets any one of the rules will be filtered and included in the result.

For example, if the logical relationship is ((1 And 2) Or 3) in the Basic Filter Condition area, the contents that meet both the filter rule 1 and filter rule 2, or meet the filter rule 3, will be filtered out.

You can view the logical relationship of the filter rules in the **Basic Filter Condition** area.

- **Specify the time range of the scanned files to display in the report** – Select one of the following options:
  - **All time** – The files in all of the time range will be displayed in the report.
  - **Specify scan time range** – Select this radio button to define specified time range. Select the calendar ( ) button, the time range calendar appears. Specify the time range, and then select **OK**.
- **Customize Exported Report** – Configure the report's customized settings:
  - **Header Image** – Select **Browse** to select a header image. Select **Reset** to clear your selected image and return to displaying the default image.
  - **Alt Text for Header** – Enter the alt text for the header image.
  - **Footer Image** – Select **Browse** to select a footer image. Select **Reset** to clear your selected image and return to displaying the default image.
  - **Alt Text for Footer** – Enter the alt text for the footer image.

Using Profile Manager for Exporting Report to HTML

After you finish configuring the export report settings, select **Export**. An **Export To** pop-up window appears. Enter a profile name, and then select **OK**. The **Profile Manager** tab appears and the profile displays under the **Profile Manager** tab. You can go to the **Profile Manager** tab by selecting **Profile Manager** in the **Export All Requests to HTML** interface.

Under the **Profile Manager** tab, all of the Export Report to HTML profiles are displayed.

You may perform any of the following actions on a selected profile:

- **View** – Select **View** to see the detailed configuration information of the selected profile.
- **Edit** – Select **Edit** to edit the detailed configuration information of the selected profile.
- **Delete** – Select **Delete** to delete the selected profiles.
- **Run Now** – Select **Run Now** to run the profile immediately. A pop-up message appears to prompt you to go to the **Export Requests** interface for details. In the **Export Requests** interface, you can view the job status. After the job finishes, select **Download** to download the exported report to the specified location.

Viewing the Exported HTML Report

After you download the exported report ZIP file, extract the ZIP file, and then locate the **index.html** file. Open the **index.html** file to view the report.

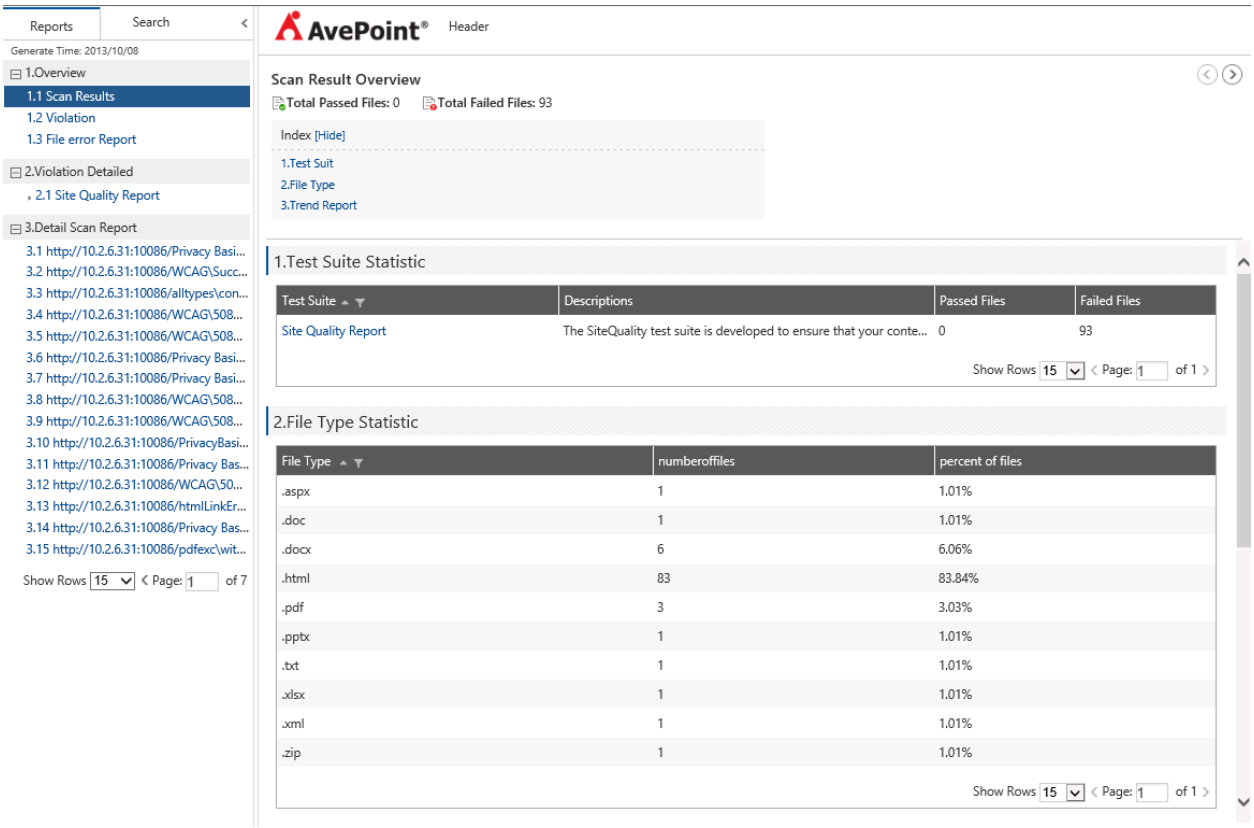

Figure 17: The Exported HTML Report.

Classification Scanner

Classification Scanner allows you to perform a scheduled or immediate job to scan the related SharePoint Online sites content using the defined rule. You can then take action on the scanned content.

Getting Started

Refer to the sections below for important information on getting started with Classification Scanner.

Launching Classification Scanner

To launch Classification Scanner, complete the following steps:

1. Log into Compliance Guardian Online.
2. Select **Classification Scanner** to launch its interface.
3. If you are already in the software, select **Scanner** on the top of the interface, and then select **Classification Scanner** from the drop-down list.

Managing Scans

In the **Classification Scanner** interface, you will see a list scans.

You may perform any of the following actions on a selected scan:

- **Create** – Select **Create** to create a new scan. Refer to the Creating Scans section for the details.
- **View** – Select **View** to see the details of the selected scan. In the View Scan interface, select **Scan Now** to scan immediately. Here you can also select **Edit** to make changes to the scan's settings. You will be brought to the **Edit** page where you can change the settings for this scan. After editing the settings, select the down arrow ( ) after **Save**, a drop-down list appears. Select **Save** in the drop-down list to save the changes; to save a changed scan as a new one, select **Save As**; select **Save and Scan Now** in the drop-down list to save the scan and run immediately. At any time, select **Cancel** to return to the **Classification Scanner** interface without saving any of your changes.
- **Edit** – Select **Edit** to make changes to the selected scan's settings. You will be brought to the **Edit** page where you can change the settings for this scan. Select the down arrow ( ) next to **Save**. A drop-down list appears. Select **Save** in the drop-down list to save the changes; to save a changed scan as a new one, select **Save As**; select **Save and Scan Now** in the drop-down list to save the scan and run immediately. At any time, select **Cancel** to return to the **Classification Scanner** without saving any of your changes.
- **Delete** – Select **Delete** to delete the selected scans. A warning message will appear to confirm the deletion. Select **OK** to delete the selected plan, or select **Cancel** to return to **Compliance Scanner** interface without deleting the selected scans.

- **Scan** – Run the selected scan immediately.

Creating Scans

Currently Classification Scanner only supports scanning content in SharePoint Online sites. To create a new scan, select **Create**. Then, select **For SharePoint Online** in the drop-down list. The Create Scan interface appears.

***Note**: If you have a trial license, the maximum number of SharePoint Online items that can be scanned in one scan is 100.

Selecting Authentication Profile

You must first select an authentication profile to connect to the Office 365 admin center. In the upper-left corner of the Create Scan interface, select an authentication profile from the **Select an Authentication Profile** drop-down list. You can also select **New Authentication Profile** to create a new one. Select **Refresh** to refresh the authentication profile in the drop-down list.

Defining the SharePoint Online Site Scope

There are two methods for getting the SharePoint Online Site scope:

- **Automatically Discover SharePoint Online Sites** – Select this radio button in the left pane of the Create Scan interface, and then select **My Registered Sites**. Compliance Guardian Online will connect to Office 365 admin center and scan all of the site collections using the account specified in the selected authentication profile. Then, all of the SharePoint Online site collections will be listed under the **My Registered Sites** node.

  ***Note**: If **Automatically Discover SharePoint Online Sites** is selected, the user in the selected authentication profile must have the site collection administrator permission to the target site collections, must have the Global administrator role, and the user must apply a valid SharePoint Online license.

- **Manually Enter SharePoint Online Site** – Select this radio button in the left pane of the Create Scan interface, a text box appears. Enter a SharePoint Online site collection and then select **My Registered Sites** node, the entered site collection is displayed under the **My Registered Sites** node.

  ***Note**: The entered site collection must exist in the connected Office 365 admin center.

  If **Manually Enter SharePoint Online Site** is selected, the user in the selected authentication profile must have the site collection administrator permission to the target site collections, and must apply a valid SharePoint Online license.

After getting the SharePoint Online sites, select the SharePoint Online site collection that you want to scan under the **My Registered Sites** node. You can also select the nodes under the site collection to scan.

If you want to scan the posts and replies in Newsfeed, you must select the **MicroFeed** list under a site.

If you want to scan the user profile, select the personal site collection, and deselect the top-level site node and the nodes under the top-level site node.

Configuring Scan Settings

In the right pane of the Create Scan interface, configure the following settings:

- **Tagging Test Suite Selection** – Select the tagging test suites. The SharePoint Online sites will be scanned according to the rules defined in the selected test suites.
- **Action Policy** – Select an action policy from the drop-down list or create a new action policy to define the actions to the content that will be scanned For more information on working with action policies, refer to Action Policy.
- **Spider Profile** – Select the spider profile used for Classification. The SharePoint Online sites will be crawled based on the rules defined in the spider profile. Select **View** to view the settings in the selected spider profile. Select **Edit** to edit the spider profile. For the details about the spider profile, refer to Spider Profile.

Select **Save** to save the scan. A pop-up window appears. Enter the Scan Name and Share Mode, then you can save the scan by selecting **Save** in the window, or select **Save and Scan Now** to save the scan and scan immediately. Select **Cancel** in the window to exit the window.

Select **Scan Now** to scan immediately.

Select **Reset** to erase any of the configured settings in the Create Scan interface.

Select **Cancel** to exit the Create Scan interface without any changes.

Editing Scans

To modify a previously configured scan, select the scan, and then select **Edit**. For more information about editing configurations for a scan, refer to Creating Scans.

Select **Save**. A drop-down list appears. Choose from the following options:

- Select **Save** from the drop-down list to save the changes.
- Select **Save As** to save the scan as another one.
- Select **Save and Scan Now** to save the changes and scan immediately.

Classification Reports

Classification Reports includes Action Report, Incident Report and Export Requests. It is used to view the report results of the files affected by Classification Scanner actions, as well as provide operations to the quarantined files, redacted files and encrypted files.

Launching Classification Reports

To launch Classification Reports, complete the following steps:

1. Log in to Compliance Guardian Online. If you are already in the software, select **Home** on the top of the screen to go to the home page. From the home page, all of the product modules are displayed.
2. Select **Classification Reports** to launch its interface.
3. Alternatively, you can select **Reports** on the top of the screen, and select the corresponding module of **Classification Reports** on the navigation bar to launch Classification Reports.

Action Report

Action Report is used to view the results of the files affected by Classification Scanner. Select **Classification Reports** in the home page of Compliance Guardian Online, the **Action Report** interface appears, or you can select **Reports** on the top of the screen, and then select **Action Report** in **Classification Reports** to access the interface.

You must configure the **Report Settings** at the upper-right corner of the **Action Report** interface:

- **Specify a default risk formula** – Select the down arrow (), a drop-down list appears. All of the risk formulas will be loaded in the drop-down list. Select a risk formula that will be used to calculate the risk scores of a file. The default value is **Raw**.
- **Specify the range of risk levels** – Specify the risk level range by specify two values. The files whose risk scores are lower than the value you specified in the left field are considered with the low risk priority. The files whose risk scores are greater than the value you specified in the right field are considered with the high priority. The files whose risk scores are between the two specified values are considered with the medium priority. The default values are **5** and **10**.

Select **OK** to save the changes.

Selecting Scope to Generate Action Report

The SharePoint Online site collections will be loaded on the left pane of the **Action Report** interface.

To select scope for generating the action report, complete the following steps:

1. Select **My Registered Sites**, the site collections that have performed the corresponding Classification Scanner jobs will be loaded. Select the desired nodes, the corresponding action report of the files related to the selected nodes will be generated.
2. You can select a time range, the file affected by actions in the specified time range will be displayed in the action report. Select the down arrow (⌄) under the **Time Range** field, and then configure the range. Select **OK** to save the settings, or select **Cancel** without saving any changes.
3. Select **Show Report**. The action report will be displayed on the right pane of the interface. Select **Reset** to erase any settings you configured in the left pane.

Viewing Action Reports

The Action Report contains three sections: Action Overview, Risk Statistics and Reports.

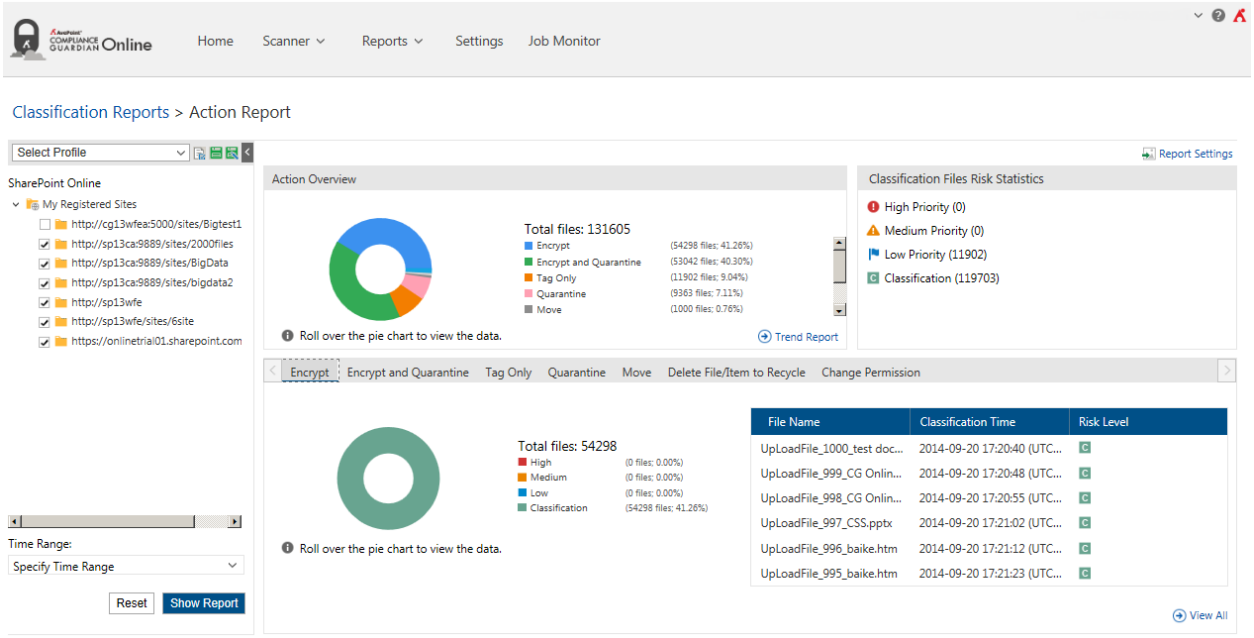

Figure 18: Action Reports interface.

Action Overview

The Action Overview section displays the proportion of the files taken a particular action. If you hover over a sector in the pie chart, you can also view the file and action information.

If you want to view the trend report of the scan results, select the **Trend Report** link and review it in the Trend Report interface. The top five actions that have the most files taken are selected in the upper-left corner of the **Trend Report** interface. The files affected by the selected actions will be displayed in a histogram. You can change the selection according to your own requirement for reviewing the desired trend report. Specify a date range from **This Month**, **Last Month**, **Last 3 Months**, **Last 6 Months**, and **Last 12 Months** to view the files in the specified time range.

Select **Back** to return to the previous **Action Report** interface.

Classification File Risk Statistics

The Classification File Risk Statistics section displays the number of the files in each priority level. The files are classified according to their risk scores that are calculated by the selected risk formula.

However, there are two cases when a file in the Classification File Risk Statistics section does not have a risk value.

- The file is scanned but the **NoRisk** option was selected when configuring the test suite. (i.e. The test suite's **NoRisk** attribute value is **True**).
- The file was selected based on action rather than content. In this case, the file was not scanned so it does not have a risk score.

Reports

The **Reports** section displays the report of the files taken a particular action. Select the action tab, the result report of the files taken this action will be displayed. A pie chart is displayed at the lower-left corner of the field displaying the risk information of the files that taken the particular action. Hover over a sector in the pie chart, you can also view the file and risk level information.

Select **View All** to view the information on all of the files affected by the particular action. Then you can view the File Name, Classification Time, Risk Level and Details. Select the details ( ) button, the detailed information of the corresponding file is displayed in the window.

- **File Name** – The name of the corresponding file.
- **Original Location** – The full URL of the specified file. Selecting the URL in this area will direct you to the specified file.
- **Action Information** – The information of the actions taken to the file, as well as the risk level, the status of taking actions, and the time of taking actions.
- **Tagging Information** – The tag information, including the tag name, tag value, the status of adding the tag, and the position of the tag.
- **Scan Information** – The scan name applied to the file, and the related test suite information.

You can customize how these files are displayed in the following ways:

- **Search** – Filter the files and display them by the keyword you designate. The keyword must be contained in a column value. At the top-right corner of the viewing pane, enter the keyword for the files you want to display in the text box that appears after you select the search ( ) button.
- **Sort –** Select the header row of each column to sort all of the values in the specified column according to the ascending/descending order.
- **Filter the column** ( ) – Select the button on the header row of the **Risk Level** column to filter which item in the list is displayed. Unlike Search, you can filter whichever item you

want, rather than search based on a keyword. Hover over the column name you want to filter, then select the filter the column button (), and then select the checkbox next to the item name to have that item shown in the list.

- To change the number of files displayed per page, select the desired number from **10** (default value), **15**, **20**, **30** in the **Show rows** drop-down menu at the lower-right corner.
- To go to the specified page, enter the page number in the **Go to … of** text box at the lower-right corner and press **Enter**.
- To go to the next page, select the **>** button at the lower-right corner; to return to the previous page, select the **<** button at the lower-right corner.

To export the results, select the **Export to Datasheet** link on the upper-right corner of this interface and then enter a request name in the **Export To** window. Then select **OK**, and the detailed information displayed on this page will be exported to a CSV file for further use.

Select **Back** on the upper-right corner to return to the **Action Report** interface.

Configuring Settings for Action Report

The following settings can be configured in the Action Report interface:

- **Save Displayed Action Report** – If you want to save the currently displayed report, enter a profile name in the text box at the top of the left pane, and then select the Save () button. The currently displayed report will be saved, the next time you access Action Report, you can select it from the drop-down list at the top of the left pane directly, and then the corresponding report will be displayed. You can also select the Save As () button at the top of the left pane. Then, enter a profile name in the pop-up window and select **OK**. The profile will be saved.
- **Set Displayed Action Report as Default** – If you want to set the displayed report as the default report which will be directly displayed the next time you access Action Report, select a profile in the drop-down list at the top of the left pane, and then select the Set as Default () button.

Incident Manager

Incident Manager allows you to manage and performed some specified actions to the quarantined files, encrypted files, and redacted files. Select **Reports** on the top of the screen, and then select **Incident Manager** in Classification Reports to access the Incident Manager interface.

***Note**: The files that are affected by the corresponding actions within seven days are loaded in Incident Manager. You can change the filter condition to view more files.

Managing Quarantined Files

The **Quarantine** tab is selected by default when you go into the **Incident Manager** interface. All of the quarantined files are displayed in the interface.

Filtering Files

You can decide which files are displayed in the interface under the **Quarantine** tab by configuring the filter conditions. Select **Filter** above the table listing quarantined files, a window appears. Configure the filter conditions in the window:

- **Time Range** – Select the time range.
- **Site Collection** – The SharePoint online site collections that contain the out of place quarantined files or in place quarantined files will be loaded. Select the down arrow ( ) after the **Site Collection** box. Then, select the site collections from the drop-down list, and select **OK**.

Select **Show Data**. All of the quarantined files that meet the above configured filter conditions will be displayed in the interface. Select **Cancel** to exit the window without saving any changes.

Managing File Content

To manage a file's content, select the file, and then select **Manage Content** above the table listing quarantined files. Then, the following actions in a drop-down list, which can be performed to a quarantined file:

- **Download** – View the selected file's content.
    - For the SharePoint files or items that are affected by the **In place quarantine** method, after you select **Download** in the drop-down list:
        - You can view the files on SharePoint site webpage.
        - You can directly edit the content of the file.
        - SharePoint items cannot be performed this action.
    - For the SharePoint files or items that are affected by the **Out of place quarantine** method, after you select **Download** in the drop-down list:
        - The file will be downloaded.
        - SharePoint items cannot be performed this action since there is no content in an item.
- **Upload** – Upload a file.
    - For the SharePoint files or items that are affected by the **In place quarantine** method, after you select **Upload** in the drop-down list: Since the files or attachments of items that are affected by the **In place quarantine** method are

edited in the webpage directly, this **Upload** function does not take effect on these files and items.

- For the SharePoint files or items that are affected by the **Out of place quarantine** method, after you select **Upload** in the drop-down list:
  - The downloaded and edited file will be uploaded and will replace the selected file.

    ***Note:** The uploaded file name and file type must be same as those of the selected file.

  - The downloaded and edited attachment of the SharePoint item can be uploaded and replace the original attachment of the item.

    ***Note:** The uploaded attachment name and type must be same as the original attachment name and type.

  Users must download the file for reviewing the violations in the file, and then edit the file according to their own requirement. Then, upload the edited file to **Compliance Guardian Online** > **Incident Manager** > **Quarantine**. Users can restore the edited file to the original place from the quarantined location through Compliance Guardian Online.

- **View Version History** – View the version history of a file or an item.
  - For the SharePoint files or items that are affected by **the In place quarantine** method, after you select **View Version History** in the drop-down list, the corresponding SharePoint webpage appears displaying the file or item's version history.
  - For the SharePoint files or items that are affected by the **Out of place quarantine** method, after you select **View Version History** in the drop-down list, all of the file or item versions are displayed in the **View Version History** page. You can perform the following actions to a selected version:
    - **Download** – Select a version, and then select **Download** on the ribbon to download the file or item's version for reference.
    - **Restore** – Select a version of the selected file or item, then you can select **Restore** to restore the current version of the file or item. For detailed information, refer to Restoring Files.
    - **Delete** – Select one or more file or item's versions, and then select **Delete** on the ribbon to delete the selected versions.

      ***Note**: The current file or item version cannot be deleted.

  Select the Close ( ) button to exit the **View Version History** page.

- **View Properties** – View the file or item's properties.

- For the SharePoint files or items that are affected by the **In place quarantine** method, after you select **View Properties** in the drop-down list:
    - The corresponding SharePoint webpage appears displaying the file's properties.
    - The corresponding SharePoint webpage appears displaying the item's properties. You can open the item attachment in the SharePoint webpage, and then edit the content of the attachment.
- For the SharePoint files or items that are affected by the **Out of place quarantine** method, after you select **View Properties** in the drop-down list:
    - All of the selected file's properties are displayed in the **View Properties** page. Select **Close** to exit the **View Properties** page.
    - All of the selected item's properties are displayed in the **View Properties** page. You can select the attachment name to download the attachment of the item, and edit the content of the attachment, and then upload the edited item through the **Upload** function which is introduced above. You can also delete the attachment in the page. Select **Close** to exit the **View Properties** page.

Restoring Files

You can restore a quarantined file or item by selecting **Restore** above the table listing quarantined files.

Restoring the SharePoint Online Files or Items that Are Affected by the In Place Quarantine Method

After you select a SharePoint file or item that is affected by the **In place quarantine** method, configure the following settings in the **Restore** interface:

- **Options –** Configure the options:
    - **Ignore this file until the file or rules change** – Select this checkbox, the file or item will not be scanned after it is restored until the test suite or action policy is changed, or until the file or item is changed.
    - **Change classification result** – The checkbox is enabled if you select **Ignore this file until the file or rules change**. Select to change the classification result by selecting the **Change classification result** checkbox. A table listing all the tags that have been added to the file or item appears. You can change the tags based on your own requirement. The file or item will also have the default risk values of the changed tag.
- **Conflict Resolution** – If there is a file (this function will not be taken effect on a SharePoint item) whose name is same as the file name that you want to restore in the destination, a conflict will be judged. Select a conflict resolution:
    - **Replace** – The conflicted destination file will be replaced with the selected file after the restore.

- **Skip** – The file will be skipped to restore to the destination.

Select **OK** to save the changes, or select **Cancel** to exit the interface without saving any changes.

Restoring the SharePoint Online Files or Items that Are Affected by the Out of Place Quarantine Method

After you select a SharePoint file or item that is affected by the **Out of place quarantine** method, configure the following settings in the **Restore** interface:

- **Restore Type** – Select **In place restore** to restore the selected file or item to its original place. Select **Out of place restore** to restore the selected file or item to another place in SharePoint.

  If you select **In place restore**:

  - **Ignore this file until the file or rules change** – Select this checkbox, the file or item will not be scanned after it is restored until the test suite or action policy is changed, or until the file or item is changed.
  - **Change classification result** – The checkbox is enabled if you select **Ignore this file until the file or rules change**. Select to change the classification result by selecting the **Change classification result** checkbox. A table listing all the tags that have been added to the file or item appears. You can change the tags based on your own requirement. The file or item will also have the default risk values of the changed tag.

  If you select **Out of place restore**: you must select an authentication profile to connect to the Office 365 admin center from the **Select an authentication profile** drop-down list. Select **Refresh** to refresh the authentication profile in the drop-down list. The SharePoint Online site collections will be loaded after you select **My Registered Sites**. Browse the desired site collection to a list level, library level, or folder level, the file or item will be restored to the selected list, library or folder.

- **Conflict Resolution** – Refer to Restoring the SharePoint Online Files or Items that Are Affected by the In Place Quarantine Method for details.

For the SharePoint files or items that are affected by the **Out of place quarantine** method, after they are restored to SharePoint, the following related objects or properties will be affected.

- **Workflow** – The original related workflows will not associate to the restored file or item.
- **ID** – The file's or item's ID will be changed after the file or item is restored to SharePoint.
- **Web part** – Refer to the following scenarios for details:
  - If the file's Web part is not saved together with the file or item (saved in the different tables in SharePoint database), the web part will not exist after the file or item is restored even if you selected **In place restore** or **Out of place restore** as the **Restore Type**.

    - If the file's Web part is saved together with the file or item (saved in the same tables in SharePoint database) and if you select **In place restore** as the Restore Type, the Web part can be restored normally along with the file or item.
    - If the file's Web part is saved together with the file or item (saved in the same tables in SharePoint database) and if you select **Out of place restore** as the **Restore Type**, the Web part may be affected after the restore.
- **Permissions** – The restored file or item will inherit its parent's permissions.
- **Rating** – The restored file or item's rating will no longer exist after it is restored.
- **Versions** – The file or item's versions will not be kept after the file or item is restored to SharePoint. Only the version count can be kept.

Deleting Quarantined Files

Select the quarantined files that you want to delete, and select **Delete** above the table displaying the quarantined files. The selected files will be permanently deleted.

Exporting Files

Select **Export to Datasheet** above the table displaying quarantined files to export the general information of all of the quarantined files.

Managing Encrypted Files

Select the **Encryption** tab to manage the encrypted files. Any encrypted or encrypted and quarantined file will display in this interface.

Filtering Files

You can decide which files are displayed in the interface under the **Encryption** tab by configuring the filter conditions. Select **Filter** above the table listing encrypted files, a window appears. Configure the filter conditions in the window:

- **Time Range** – Select the time range.
- **Site Collection** – The SharePoint online site collections that contain the encrypted files will be loaded. Select the down arrow ( ) after the **Site Collection** box. Then, select the site collections from the drop-down list, and select **OK**.

Select **Show Data**. All of the encrypted files that meet the above configured filter conditions will be displayed in the interface. Select **Cancel** to exit the window without saving any changes.

Managing File Content

To manage a file's content, select the file, and then select **Manage Content** above the table listing encrypted files. Then, the following actions in a drop-down list, which can be performed to a quarantined file:

- **Download** – View the selected file's content.
    - SharePoint files will be downloaded.
    - SharePoint items cannot be viewed since there is no content in an item.
- **Upload** – Upload a file.
    - For SharePoint files, after you select **Upload** in the drop-down list, the downloaded and edited file will be uploaded and will replace the selected file.

      ***Note:** The uploaded file name and type must be same as those of the selected file.

    - For SharePoint items, after you select **Upload** in the drop-down list, the downloaded and edited attachment of the SharePoint item can be uploaded to replace the original attachment of the item.

      ***Note:** The uploaded attachment name and type must be same as the original attachment name and type.

  Users can download the file for reviewing the violations in the file, edit the file according to their own requirement, and then upload the edited file by navigating to **Compliance Guardian Online** > **Incident Manager** > **Encryption**.

- **View Version History** – View the version history of a file or an item.
    - For the SharePoint files or items that are affected by the **Encrypt** or **In place quarantine** method, after you select **View Version History** in the drop-down list, the corresponding SharePoint webpage appears displaying the file or item's version history.
    - For the SharePoint files or items that are affected by the **Out of place quarantine** method, after you select **View Version History** in the drop-down list, all of the file or item versions are displayed in the **View Version History** page. You can perform the following actions to a selected version:
        - **Download** – Select a version, and then select **Download** on the ribbon to download the file or item's version for reference.
        - **Restore** – Select the latest version of the selected file or item, then you can select **Restore** to restore the current version of the file or item. For detailed information, refer to Restoring Files.
        - **Delete** – Select one or more file or item's versions, and then select **Delete** on the ribbon to delete the selected versions.

          ***Note**: The current file or item version cannot be deleted.

      Select the Close ( ) button to exit the **View Version History** page.

- **View Properties** – View the file or item's properties.

- For SharePoint files that are affected by the Encrypt and Quarantine action, and the Quarantine Method for the files is **In place quarantine**, after you select **View Properties**, the corresponding SharePoint webpage appears displaying the file's properties.
- For SharePoint files that are affected by the Encrypt action, after you select **View Properties**, the corresponding SharePoint webpage appears displaying the file's properties.
- For SharePoint files that are affected by the Encrypt and Quarantine action, and the Quarantine Method for the files is **Out of place quarantine**, after you select **View Properties** in the drop-down list, all of the selected file's properties are displayed in the **View Properties** page. Select **Close** to exit the View Property page.
- For SharePoint items, after you select **View Properties** in the drop-down list, all of the selected item's properties are displayed in the **View Properties** page. You can select the attachment name to download the attachment of the item, and edit the content of the attachment, and then upload the edited item through the **Upload** function which is introduced above. Select **Close** to exit the View Properties page.

Decrypting Files

You can decrypt an encrypted file or item by selecting **Decrypt** above the table listing encrypted files.

Decrypting the SharePoint Files or Items Affected by the Encrypt Action

After you select a SharePoint file or item affected by the **Encrypt** action, configure the options in the Decrypt interface:

- **Ignore this file until the file or rules change** – Select this checkbox. The file or item will not be scanned until the action policy or test suite is changed, or until the file or item is changed.
- **Change classification result** – If you have selected the **Ignore this file until the file or rules changed** checkbox, this checkbox is enabled. Select to change the classification result by selecting the **Change classification result** checkbox. A table listing all the tags that have been added to the file or item appears. You can change the tags based on your own requirement. The file or item will also have the default risk values of the changed tag.

Decrypting the SharePoint Files or Items Affected by the Encrypt and Quarantine Action (Quarantine Method is In Place Quarantine)

After you select a SharePoint file or item that is affected by the **Encrypt and Quarantine** action and the Quarantine Method is **In place quarantine**, configure the following settings in the Decrypt interface:

- **Options –** Configure the options:

- **Ignore this file until the file or rules change** – Select this checkbox. The file or item will not be scanned until the action policy or test suite is changed, or until the file or item is changed.
- **Change classification result** – If you have selected the **Ignore this file until the file or rules change** checkbox, this checkbox is enabled. You can select to change the classification result by selecting the **Change classification result** checkbox. A table listing all the tags that have been added to the file or item appears. You can change the tags based on your own requirement. The file or item will also have the default risk values of the changed tag.

- **Conflict Resolution –** If there is a file (this function will not be taken effect on a SharePoint item) whose name is same as the file name that you want to restore in the location where the file is restored, a conflict will be judged. Select a conflict resolution:
  - **Replace** – The conflicted destination file will be replaced with the selected file or item after the restore.
  - **Skip** – The file will be skipped to restore to the destination.

Decrypting the SharePoint Files or Items Affected by the Encrypt and Quarantine Action (Quarantine Method is Out of Place Quarantine)

After you select a SharePoint file or item that is affected by the **Encrypt and Quarantine** action and the Quarantine Method is **Out of place quarantine**, configure the following settings in the **Decrypt** interface:

- **Restore Type** – Select **In place restore** to restore the selected file or item to its original place. Select **Out of place restore** to restore the selected file or item to another place in SharePoint.

  If you select **In place restore**:

  - **Ignore this file until the file or rules change** – Select this checkbox, the file or item will not be scanned after it is restored until the test suite or action policy is changed, or until the file or item is changed.
  - **Change classification result** – The checkbox is enabled if you select **Ignore this file until the file or rules change**. Select to change the classification result by selecting the **Change classification result** checkbox. A table listing all the tags that have been added to the file or item appears. You can change the tags based on your own requirement. The file or item will also have the default risk values of the changed tag.

  If you select **Out of place restore**: you must select an authentication profile to connect to the Office 365 admin center from the **Select an authentication profile** drop-down list. Select **Refresh** to refresh the authentication profile in the drop-down list. The SharePoint Online site collections will be loaded after you select **My Registered Sites**. Browse the desired site collection to a list level, library level, or folder level, the file or item will be restored to the selected list, library or folder.

- **Conflict Resolution** – If there is a file (this function will not be taken effect on a SharePoint item) whose name is same as the file name that you want to restore in the destination, a conflict will be judged. Select a conflict resolution:
    - **Replace** – The conflicted destination file will be replaced with the selected file or item after the restore.
    - **Skip** – The file will be skipped to restore to the destination.

For the SharePoint files or items that are affected by the **Out of place quarantine** method, after they are restored to SharePoint, the following related objects or properties will be affected:

- **Workflow** – The original related workflows will not associate to the restored file or item.
- **ID** – The file's or item's ID will be changed after the file or item is restored to SharePoint.
- **Web part** – Refer to the following scenarios for details:
    - If the file's Web part is not saved together with the file or item (saved in the different tables in SharePoint database), the Web part will not exist after the file or item is restored no matter you select **In place restore** or **Out of place restore** as the **Restore Type**.
    - If the file's Web part is saved together with the file or item (saved in the same tables in SharePoint database) and if you select In place restore as the Restore Type, the Web part can be restored normally along with the file or item.
    - If the file's Web part is saved together with the file or item (saved in the same tables in SharePoint database) and if you select **Out of place restore** as the **Restore Type**, the Web part may be affected after the restore.
- **Permissions** – The restored file or item will inherit its parent's permissions.
- **Rating** – The restored file or item's rating will no longer exist after it is restored.
- **Versions** – The file or item's versions will not be kept after the file or item is restored to SharePoint. Only the version count can be kept.

Deleting Encrypted Files

Select the files that you want to delete, and select **Delete** above the table displaying the encrypted files. The selected files will be permanently deleted.

Exporting Files

Select **Export to Datasheet** above the table displaying encrypted files to export the general information of all of the encrypted files.

Managing Redacted Files

Select the **Redaction** tab to manage the redacted files. All of the files that are affected by the **Quarantine Before Redact** action are displayed in the interface.

Filtering Files

You can decide which files are displayed in the interface under the **Redaction** tab by configuring the filter conditions. Select **Filter** above the table listing encrypted files, a window appears. Configure the filter conditions in the window:

- **Time Range** – Select the time range.
- **Site Collection** – The SharePoint Online site collections that contain the redacted files will be loaded. Select the down arrow ( ) after the **Site Collection** box. Then, select the site collections from the drop-down list, and select **OK**.

Select **Show Data**. All of the encrypted files that meet the above configured filter conditions will be displayed in the interface. Select **Cancel** to exit the window without saving any changes.

Managing File Content

To manage a file's content, select the file, and then select **Manage Content** above the table listing redacted files. The following actions appear in a drop-down list, which can be performed to a redacted file:

- **Download** – View the selected file's content. For the SharePoint files or items, after you select **Download** in the drop-down list:
  - The file will be downloaded.
  - SharePoint items cannot be performed this action since there is no content in an item.
- **Upload** – Upload a file. For the SharePoint files or items, after you select **Upload** in the drop-down list:
  - The downloaded and edited file will be uploaded and will replace the selected file.

    ***Note:** The uploaded file name and type must be the same as those of the selected file.
  - The downloaded and edited attachment of the SharePoint item can be uploaded and replace the original attachment of the item.

    ***Note:** The uploaded attachment name type must be same as the original attachment name and type.

  Users always first download the file for reviewing the file, and then edit the file according to their own requirement. Upload the edited file to **Compliance Guardian Online** > **Incident Manager** > **Redaction**. Users can restore the original file that is not redacted from the quarantined location through Compliance Guardian Online.
- **View Version History** – View the version history of a file or an item.

For the SharePoint files or items, after you select **View Version History** in the drop-down list, all of the file or item versions are displayed in the **View Version History** page. You can perform the following actions to a selected version:

- **Download** – Select a version, and then select **Download** on the ribbon to download the file or item's version for reference.
- **Restore** – Select the version of the selected file or item, then you can select **Restore** to restore the current version of the file or item. For detailed information, refer to Restoring Files.
- **Delete** – Select one or more file or item's versions, and then select **Delete** on the ribbon to delete the selected versions.

  ***Note**: The current file or item version cannot be deleted.

  Select **Close** to exit the **View Version History** page.

- **View Properties** – View the file or item's properties.

  For the SharePoint files or items, after you select **View Properties** in the drop-down list:

  - All of the selected file's properties are displayed in the **View Properties** page. Select **Close** to exit the View Property page.
  - All of the selected item's properties are displayed in the **View Properties** page. You can select the attachment name to download the attachment of the item, and edit the content of the attachment, and then upload the edited item through the **Upload** function which is introduced above. Select **Close** to exit the **View Properties** page.

Restoring Files

The files or items that are affected by the **Redact and Quarantine** action are first to be backed up, the backed up files are quarantined, and then the original files are redacted. You can restore a redacted file or item to the original one by selecting **Restore** above the table listing redacted files.

After you select a SharePoint Online file or item, configure the following settings in the **Restore** interface:

- **Restore Type** – Select **In place restore** to restore the original file or item that is not redacted to its original place. Select **Out of place restore** to restore the original file or item that is not redacted to another place in SharePoint Online.

  If you select **In place restore**:

  - **Ignore this file until the file or rules change** – Select this checkbox, the file or item will not be scanned after it is restored until the test suite or action policy is changed, or until the file or item is changed.

- **Change classification result** – The checkbox is enabled if you select **Ignore this file until the file or rules change**. Select to change the classification result by selecting the **Change classification result** checkbox. A table listing all the tags that have been added to the file or item appears. You can change the tags based on your own requirement. The file or item will also have the default risk values of the changed tag.

If you select **Out of place restore**: you must select an authentication profile to connect to the Office 365 admin center from the **Select an authentication profile** drop-down list. Select **Refresh** to refresh the authentication profile in the drop-down list. The SharePoint Online site collections will be loaded after you select **My Registered Sites**. Browse the desired site collection to a list level, library level, or folder level, the file or item will be restored to the selected list, library or folder.

- **Conflict Resolution** – If there is a file (this function will not be taken effect on a SharePoint item) whose name is same as the file name that you want to restore in the destination, a conflict will be judged. Select a conflict resolution:
  - **Replace** – The conflicted destination file will be replaced with the selected file or item after the restore.
  - **Skip** – The file will be skipped to restore to the destination.

For the SharePoint files or items that are affected by the **Out of place quarantine** method, after they are restored to SharePoint, the following related objects or properties will be affected:

For SharePoint On-premises:

- **Workflow** – The original related workflows will not associate to the restored file or item.
- **ID** – The file's or item's ID will be changed after the file or item is restored to SharePoint.
- **Web part** – Refer to the following scenarios for details:
  - If the file's Web part is not saved together with the file or item (saved in the different tables in SharePoint database), the Web part will not exist after the file or item is restored even if you selected **In place restore** or **Out of place restore** as the **Restore Type**.
  - If the file's Web part is saved together with the file or item (saved in the same tables in SharePoint database) and if you select **In place restore** as the Restore Type, the Web part can be restored normally along with the file or item.
  - If the file's Web part is saved together with the file or item (saved in the same tables in SharePoint database) and if you select **Out of place restore** as the **Restore Type**, the Web part may be affected after the restore.
- **Permissions** – The restored file or item will inherit its parent's permissions.
- **Rating** – The restored file or item's rating will no longer exist after it is restored.
- **Versions** – The file or item's versions will not be kept after the file or item is restored to SharePoint. Only the version count can be kept.

Deleting Encrypted Files

Select the files that you want to delete, and select **Delete** above the table displaying the redacted files. The selected files will be permanently deleted.

Exporting Files

Select **Export to Datasheet** above the table displaying redacted files to export the general information of all of the redacted files.

Export Requests

Select **Reports** on the top of the screen, and then select **Export Requests** in Classification Reports to access the **Export Requests** interface. For more information on Export Requests, refer to Export Requests.

Job Monitor

Job Monitor allows you to view the status or details of jobs, download reports, and manage the jobs all from a central interface.

***Note**: If you have a trial license, you can only run 100 jobs in total using Job Monitor

Getting Started

Refer to the following sections for important information on getting started with Job Monitor.

Launching Job Monitor

To launch Job Monitor and access its functionality, log in to Compliance Guardian Online. Select **Job Monitor** to launch its interface. If you are already in the software, select **Job Monitor** on the top of the interface.

Managing Jobs

In the **Job Monitor** interface, you will see a list of the scan jobs.

You may perform any of the following actions on a selected job:

- **Download** – Select a job, and then select **Download** to download the job report. A pop-up window appears. Select **TXT**, **CSV** or **XLS** as the format for the report in the **Select the downloaded report format:** drop-down list. Then select **Download** to download the report, or **Cancel** to return to the **Job Monitor** interface.
- **View** – View a job report of the selected job. Select the job by selecting the corresponding checkbox. Select **View** on the ribbon. The **View Job Details** interface appears. The job report displayed in the interface with the **Summary** tab selected. The **Summary** tab displays general information about the job. For more in-depth information, select the corresponding **Details** tabs in the viewing pane. You can also download the job report by selecting Download in the **View Job Details** interface.
- **Stop** – Stop the selected running jobs.
- **Delete** – Select **Delete** to delete the job information of the selected jobs.

Appendix A: Accessing Hot Key Mode

In order to work faster and improve your productivity, Compliance Guardian Online supports hot key mode for you to perform corresponding actions quickly using your keyboard. To access hot key mode in the Compliance Guardian Online interface, press **Alt** on your keyboard.

For different browsers, the methods for performing the Compliance Guardian Online functions using hot key are different. Refer to the following table for details.

Browsers	Methods Using Hot Key
Internet Explorer	Alt + Hot Key, and then press Enter
Firefox	Alt + Shift + Hot Key
Chrome	Alt + Hot Key
Safari	Alt + Hot Key

The following table provides a list of hot keys for the top level in Compliance Guardian Online.

Operation Interface	Hot Key
Compliance Guardian Online Home Page	O
Scanner	P
Reports	R
Settings	I
Job Monitor	J
User	L

Compliance Scanner Page

The following table provides a list of hot keys for the functionalities of the **Compliance Scanner** page.

<table>
<tr><th colspan="6">Functionality Name and Hot Key</th></tr>
<tr><td rowspan="4">Create</td><td rowspan="4">G</td><td>Save</td><td colspan="3">N</td></tr>
<tr><td>Scan Now</td><td colspan="3">G</td></tr>
<tr><td>Reset</td><td colspan="3">K</td></tr>
<tr><td>Cancel</td><td colspan="3">W</td></tr>
<tr><td rowspan="3">View</td><td rowspan="3">M</td><td>Scan Now</td><td colspan="3">Q</td></tr>
<tr><td rowspan="2">Edit</td><td rowspan="2">K</td><td>Save</td><td>Q</td></tr>
<tr><td>Cancel</td><td>W</td></tr>
<tr><td>Close</td><td colspan="3">W</td></tr>
<tr><td rowspan="2">Edit</td><td rowspan="2">K</td><td>Save</td><td colspan="3">Q</td></tr>
<tr><td>Cancel</td><td colspan="3">W</td></tr>
<tr><td>Delete</td><td colspan="5">N</td></tr>
<tr><td>Scan</td><td colspan="5">Q</td></tr>
</table>

Compliance Reports

The following table provides a list of hot keys for **Compliance Reports** page functionalities.

Functionality Name and Hot Key	
Scan Filter	M
Trend Report	N
Export to Datasheet	K

Scan Result

The following table provides a list of hot keys for the **Scan Result** page functionalities.

Functionality Name and Hot Key	
Passed Files	G
Failed Files	Q
View Detailed Report Page	
Detailed Report	U
Error Highlight Report	W

Human Auditor

The following table provides a list of hot keys for the **Human Auditor** page functionalities.

Functionality Name and Hot Key	
Change Status	N
Auditing History	Y

Export Requests

The following table provides a list of hot keys for the **Export Requests** page functionalities.

Functionality Name and Hot Key	
Download	W
Delete	N
Stop	Q
Restart	K

Export All Requests to HTML

The following table provides a list of hot keys for the **Export All Requests to HTML** page functionalities.

Functionality Name and Hot Key			
Export Report Settings	Q		
Export	G		
Cancel	W		
Profile Manager	U		
View	M	Edit	K
		Cancel	W
Edit	K	Save	Q
		Cancel	W
Delete	N		
Run Now	W		

Classification Scanner Page

The following table provides a list of hot keys for the **Classification Scanner** page functionalities.

Functionality Name and Hot Key					
Create	G	Save	N		
		Scan Now	G		
		Reset	K		
		Cancel	W		
View	M	Scan Now	Q		
		Edit	K	Save	Q
				Cancel	W
		Close	W		
Edit	K	Save	Q		
		Cancel	W		
Delete	N				
Scan	Q				

Classification Reports

The following table provides a list of hot keys for the **Classification Reports** page functionalities.

Functionality Name and Hot Key	
Action Report Page	
Profile Selection	M
Export to Datasheet	K
Incident Manager	

Functionality Name and Hot Key	
Quarantine tab	Q
Filter	W
Export to Datasheet	K
Encryption tab	U
Filter	W
Export to Datasheet	K
Redaction tab	Y
Filter	W
Export to Datasheet	K

Export Requests

The following table provides a list of hot keys for the **Export Requests** page functionalities.

Functionality Name and Hot Key	
Download	W
Delete	N
Stop	Q
Restart	K

Preference

The following table provides a list of hot keys for the **Preference** page functionalities.

Functionality Name and Hot Key	
Apply	Y
Reset	G

License Manager

The following table provides a list of hot keys for the **License Manager** page functionality.

Functionality Name and Hot Key	
Extend License	G

Compliance Guardian Online Auditor

The following table provides a list of hot keys for the **Compliance Guardian Online Auditor** page functionality.

Functionality Name and Hot Key	
Export to Datasheet	K

Auditor Settings

The following table provides a list of hot keys for the **Auditor Settings** page functionalities.

Functionality Name and Hot Key	
Apply	Y
Audited Actions	G

Group Management

The following table provides a list of hot keys for the **Group Management** page functionalities.

Functionality Name and Hot Key					
Create	G	Add Users	G		
		Cancel	W		
		Save	Q		
		Cancel	N		
View	M	Edit	K	Save	Q
				Cancel	N
		Close	W		
Edit	K	Save	Q		
		Cancel	N		
Delete	N				

User Management

The following table provides a list of hot keys for the **User Management** page functionalities.

Functionality Name and Hot Key					
Invite User	U	Send	M		
		Cancel	W		
View	M	Edit	K	Save	Q
				Cancel	W
		Close	W		
Edit	K	Save	Q		
		Cancel	W		
Delete	N				
Add to Group	G				
Re-send Invitation	Q				

Spider Profile

The following table provides a list of hot keys for the **Spider Profile** page functionalities.

Functionality Name and Hot Key					
Create	G	Save	Q		
		Cancel	W		
View	M	Edit	K	Save	Q
				Save As	U
				Cancel	W
		Close	W		
Edit	K	Save	Q		
		Save As	U		
		Cancel	W		
Delete	N				

Test Suite Manager

The following table provides a list of hot keys for the **Test Suite Manager** page functionalities.

Functionality Name and Hot Key					
Upload	Y				
Download	W				
View	M	Edit	K	Save	Q
				Save As	U
				Cancel	W
		Close	W		
Edit	K	Save	Q		
		Save As	U		
		Cancel	W		
		XML Format	M		
		Text Format	G		
Delete	N				

Check Manager

Functionality Name and Hot Key					
Upload	Y				
Download	W				
View	M	Edit	K	Save	Q
				Save As	U

Functionality Name and Hot Key					
				Cancel	W
		Close	W		
Edit	K	Save	Q		
		Save As	U		
		Cancel	W		
		XML Format	M		
		Text Format	G		
Delete	N				

Filter Policy

The following table provides a list of hot keys for the **Filter Policy** page functionalities.

Functionality Name and Hot Key					
Create	G	Save	Q		
		Cancel	W		
View	M	Edit	K	Save	Q
				Save As	U
				Cancel	W
		Close	W		
Edit	K	Save	Q		
		Save As	U		
		Cancel	W		
Delete	N				

Action Policy

The following table provides a list of hot keys for the **Action Policy** page functionalities.

Functionality Name and Hot Key					
Create	G	Save	Q		
		Cancel	W		
View	M	Edit	K	Save	Q
				Save As	U
				Cancel	W
		Close	W		
Edit	K	Save	Q		
		Save As	U		
		Cancel	W		
Delete	N				

User Agent Profile

The following table provides a list of hot keys for the **User Agent Profile** page functionalities.

Functionality Name and Hot Key					
Create	G	Save	Q		
		Cancel	W		
View	M	Edit	K	Save	Q
				Save As	U
				Cancel	W
		Close	W		
Edit	K	Save	Q		
		Save As	U		
		Cancel	W		
Delete	N				

Authentication Profile

The following table provides a list of hot keys for the **Authentication Profile** page functionalities.

Functionality Name and Hot Key					
Create	G	Save	Q		
		Cancel	W		
View	M	Edit	K	Save	Q
				Save As	U
				Cancel	W
		Close	W		
Edit	K	Save	Q		
		Save As	U		
		Cancel	W		
Delete	N				

User Notification Profile

The following table provides a list of hot keys for the **User Notification Profile** page functionalities.

Functionality Name and Hot Key					
Create	G	Save	Q		
		Cancel	W		
View	M	Edit	K	Save	Q
				Save As	U
				Cancel	W
		Close	W		

Functionality Name and Hot Key					
Edit	K	Save	Q		
		Save As	U		
		Cancel	W		
Delete	N				

Alert Profile

The following table provides a list of hot keys for the **Alert Profile** page functionalities.

Functionality Name and Hot Key					
Create	G	Save	Q		
		Cancel	W		
View	M	Edit	K	Save	Q
				Save As	U
				Cancel	W
		Close	W		
Edit	K	Save	Q		
		Save As	U		
		Cancel	W		
Delete	N				

Security Profile

Functionality Name and Hot Key					
Create	G	Save	Q		
		Cancel	W		
View	M	Edit	K	Save	Q
				Save As	U
				Cancel	W
		Close	W		
Edit	K	Save	Q		
		Save As	U		
		Cancel	W		
Delete	N				

E-mail Template

The following table provides a list of hot keys for the **E-mail Template** page functionalities.

Functionality Name and Hot Key					
Create	G	Save	Q		
		Cancel	W		
View	M	Edit	K	Save	Q
				Save As	U
				Cancel	W
		Close	W		
Edit	K	Save	Q		
		Save As	U		
		Cancel	W		
Delete	N				

Job Monitor

The following table provides a list of hot keys for the **Job Monitor** page functionalities.

Functionality Name and Hot Key	
Download	W
View	M
Stop	Q
Delete	N

Appendix B: Using Transaction Capture

Compliance Guardian Online Transaction Capture is used to record the webpages that you access, and then you can save the recorded results as a transaction file, which is used by Compliance Scanner in Compliance Guardian Online. The recorded URLs in the transaction file will be the start URLs used in Compliance Guardian Online scans.

***Note**: Make sure Microsoft .NET Framework 4.0 or a later version is installed before using Compliance Guardian Online Transaction Capture.

Getting Started to Use the Tool

Refer to the following step to get started to use the tool:

1. Download the Compliance Guardian Online Transaction Capture installation file by selecting **Download Compliance Guardian Online Transaction Capture** in the **Compliance Scanner** > **Create a Scan** or **Compliance Scanner** > **Edit Scan** interface.
2. Save the **TransactionCapture_{Version}.zip** file.
3. Unzip the **TransactionCapture_{Version}.zip** file. Then, find **TransactionCapture.exe** in the folder.
4. Right-click **TransactionCapture.exe**, and then select **Run as administrator** to open the tool.

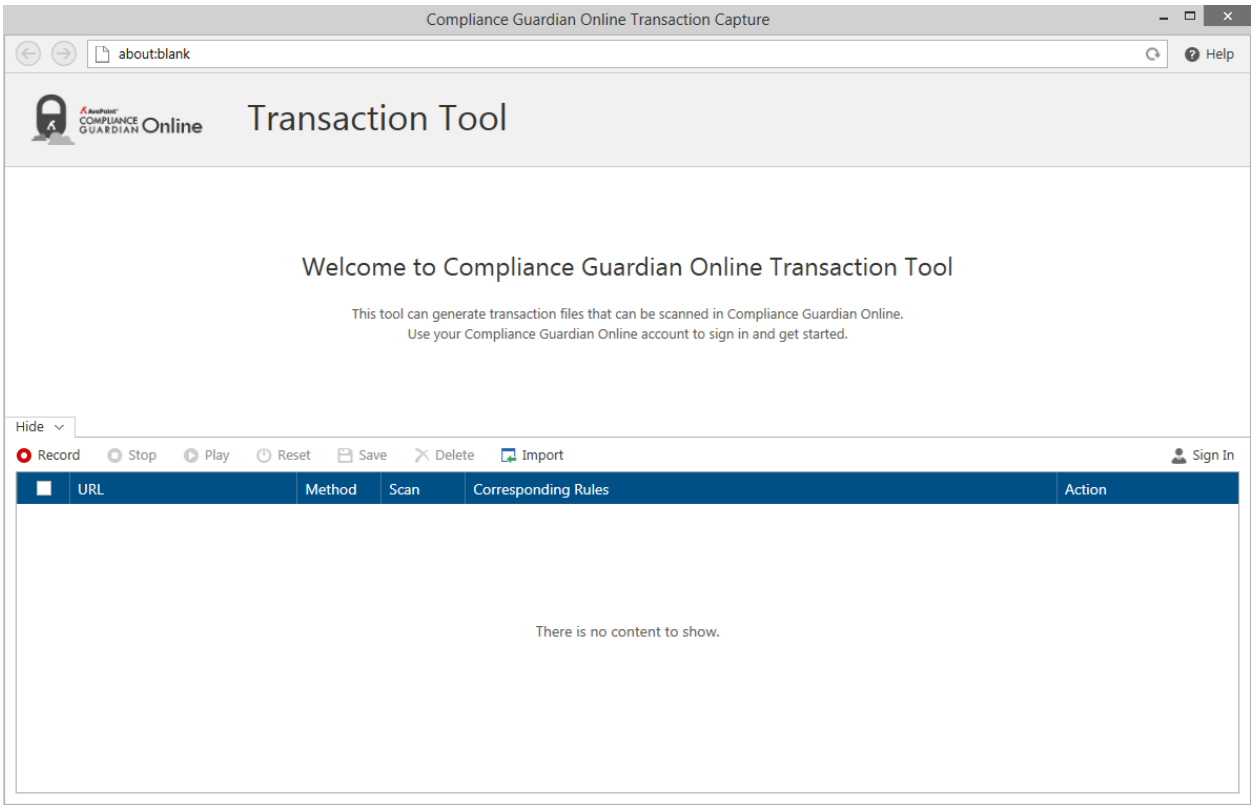

Figure 19: Compliance Guardian Online Transaction Capture interface.

Signing in the Tool

If you use your Compliance Guardian Online account to sign in the tool, you can select the desired test suites or checks to scan each URL respectively instead of selecting test suites in Compliance Scanner as the rules to scan all of the URLs in the transaction file.

Complete the following steps to sign in the tool.

1. Select **Sign In** in the tool interface. The **Sign In** window appears.
2. Enter your login ID and password (the account used to sign in Compliance Guardian Online).
3. Select **Login**.

Using the Tool

Enter the URL in the URL field on the top of the tool screen, direct to the desired page, and then you can perform the related functions using the tool. Refer to the following details about the tool functions.

- **Operation Field** – You can perform the following actions in this field:
  - **Record** – On the webpage you want to record, select the **Record** button. Compliance Guardian Online Transaction Capture will then start to record the webpages you access from this current webpage. The URLs that are recorded will be displayed on the **Recorded Information Field**.
  - **Stop** – Select the **Stop** button to stop recording the webpages.
  - **Play** – Select the **Play** button. The series of webpages that you have recorded will automatically play as they are accessed.
  - **Reset** – Select the **Reset** button, all the recorded results will be cleared up.
  - **Save** – Select the **Save** button to save the series of operation results as a transaction file. After select the **Save** button, the **Save As** window pops up. Select a location, and then select **Save** on the **Save As** window to save the transaction file, which will be used for Compliance Guardian Online Website Scanner.
  - **Delete** – Select a record in the **Recorded Information Field**, and select **Delete**, the record then will be deleted.
  - **Import** – Import a previously saved transaction file. You can view the results that the transaction file records by selecting **Play**.
- **Recorded Information Field** – The recorded results will be displayed in this field:
  - **URL** – The webpage URLs that have been recorded.
  - **Method** – The method that HTTP defines.

- **Scan** – Select the checkboxes under this column. The corresponding URL will be signed. After you save the related transaction file for Compliance Scanner, only the URLs that are signed here can be used as the Start URLs to be scanned.
- **Corresponding Rules** – The corresponding rules are only available when you sign in the tool. Select the URL, and select the drop-down list of this column. Then, select the test suites or checks used for scanning the URL.

  ***Note**: If you select the rules for a URL in the tool, you must select test suites or checks for all of the URL in the tool used for Compliance Scanner. If you select rules in the tool, the test suites in the scan policy of Compliance Scanner will not be used for scanning URLs in the generated transaction file.
- **Action** – You can edit the properties of the URL. Select **Edit Properties** in the column, the Edit Properties Field appears on the bottom of the screen:
  - **Request Headers** – Select the tab, you can edit the request header. Double-click the key or the value to edit them to your desired ones.
  - **Request Body** – Select the tab, you can edit the request body in the text field.
  - **Query String Parameters** – Select the tab, you can edit the query string parameters. Double-click the key or the value to edit them to your desired ones.

Select **Hide** or **Show** to hide or show the Operation field.

Select the close button ( ) on the top-right corner to close the Compliance Guardian Online Transaction Capture tool.

Hot Key Mode

The following table provides a list of hot keys for the functionalities of the Compliance Guardian Online Transaction Capture tool.

Functionality Name and Hot Key	
Help	Alt + F1
Hide	Alt + the up arrow in the keyboard
Show	Alt + the down arrow in the keyboard
Record	Alt + R
Stop	Alt + S
Play	Alt + P
Reset	Alt + E
Save	F12
Delete	Alt + D
Import	F11
Sign In	Alt + L
Refresh	F5

Appendix C: Test Suites and Checks

In order to provide a flexible and customizable compliance solution, AvePoint developed the AvePoint Testing Language (ATL) to provide organizations with the ability to rapidly respond to new compliance threats and requirements. ATL is an XML structured language that is used to validate and classify content related to compliance to standards or guidelines, including but not limited to security, privacy, accessibility, and content classification. Because it is open and modifiable, ATL allows for coverage to specifically match an organization's needs. ATL uses test definition files (checks) to match your environment and standards, test your framework and repair issues, validate that your content complies with organizational standards, and identify all content that requires user review and distribute a list of items to the appropriate parties.

Checks

A check is an XML file that defines the logic that Compliance Guardian Online uses to check files. Checks identify the purpose (the type of check to run, such as a pattern of characters), the condition (such as social security number pattern), and the possible result (true or false). Users can change the values in the checks to determine the check conditions, but the elements' specific format defined by Compliance Guardian Online in the checks must stay the same.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright 2001-2012 AvePoint All Rights Reserved. -->
- <Tdf TdfID="508_html_14_qaqa">
  - <ReportText>
      <Name>Section 508 1194.22 (g and h)</Name>
      <PolicyURL>http://www.access-board.gov/sec508/guide/1194.22.htm#(g)</PolicyURL>
      <Description>Identify Exception: Table row count exceeding the maximum row number. This Check can
        be customized.</Description>
      <True result="Pass">Pass, Table has less than 25 Rows.</True>
      <False result="HR">Review Required: Large table (Greater than 25 Rows) requires human
        review.</False>
    </ReportText>
  - <Element ValidWhen="true" TrueIf="All" ResultNA="NAResult" CaseSensitive="No" Name="table">
      <ListLoc Status="Warn" Type="Invalid"/>
    - <ChildElement CaseSensitive="No" Name="tr" MustExist="False">
        <ElementRepeat Alert="Yes">25</ElementRepeat>
      </ChildElement>
    </Element>
</Tdf>
```

Figure 20: Check example.

Types of Checks

Based on the different kinds of checks you can run, there are the following types of checks: FindText and ComplexFindText, RegEX and ComplexRegEX, Simple Element Validation, Find File, Web Beacon, SSL (Validation), Cookie (Validation), Dictionary Check, Enhanced Element, and Match Element Validation, FileProperty and LinkValidation.

The following lists identify the common attributes of each check.

Tdf

- **TdfID** – The ID of the check. This cannot be changed in Compliance Guardian Online Check Manager.
- **Version** – The version of the check.

ReportText

- **Name** – The name of the check. This cannot be changed in Compliance Guardian Online Check Manager.
- **PolicyURL** – The link used to provide additional information about this check, including any official rules or articles of law that specify how the check will test files.
- **True result** – Define the returning status for this check when the checking result is True. The checking logic determines whether a check result is False or True.
- **Message** – Define the message for this check when the checking result is True.
- **False result** – Define the returning status for this check when the checking result is False. The checking logic determines whether a check result is False or True.
- **Message** – Define the message for this check when the checking result is False.

Refer to the following sections for details about these types of checks.

FindText

This test type will be represented by the element <FindText>. For example:

```
<FindText CompareType="MustEqual" CaseSensitive="No" MustRepeat="1" ListLocStatus="Note"
    SearchAll="No" ListLoc="Yes" TrueIf="Found">find this</FindText>
```

Figure 21: FindText check.

It has several attributes:

- **TrueIf** – Define the condition when the check result is True. If **Found** is specified, when finding an instance, the check result of this check will be True. If **NotFound** is specified, when finding an instance, the check result of this check will be False.
- **SearchAll** – Define whether or not to check the comments and scripts.
- **ListLoc** – Define whether or not to record the instance's location in the Compliance Guardian Online database. If **Yes** is specified, then every location of the instance found will be recorded in the Compliance Guardian Online database. If **No** is specified, the check continues, but the locations of the instances found will not be recorded in the database.
- **ListLocStatus** – Define the status for the instance that is found. The status will be recorded in the Compliance Guardian Online database.

***Note:** If the status set for **True result** or **False result** is **Fail**, the value for the **Status** attribute will be **Fail**, and the value cannot be changed.

- **CaseSensitive** – Define if the text being tested for must match the case exactly.
- **MustRepeat** – Define the amount of times a word or phrase must be found before considering the condition to be True.
- **CompareType** – Define **MustContain** or **MustEqual** for this attribute.

ComplexFindText

This test type will be represented by the Element <ComplexFindText>. For example:

```
- <ComplexFindText>
    <Primary CaseSensitive="Yes" ListLocStatus="Note" ResultNA="NAResult" SearchAll="Yes"
      ListLoc="Yes" TrueIf="Found">Primary Target</Primary>
    <Secondary CaseSensitive="Yes" ListLocStatus="Note" SearchAll="Yes" ListLoc="Yes"
      TrueIf="Found"
  </ComplexFindText>
```

Figure 22: ComplexFindText check.

Primary

Configure the following attributes in this section:

- **TrueIf** – Define the condition when the check result is True. If **Found** is specified: when finding an instance, the check result of this check will be True. If **NotFound** is specified: when finding an instance, the check result of this check will be False.
- **SearchAll** – Define whether or not to check the comments and scripts.
- **ListLoc** – Define whether or not to record the instance's location in the Compliance Guardian Online database. If **Yes** is specified, every location of the instance found will be recorded in the Compliance Guardian Online database. If **No** is specified, the check continues, but the locations of the instances found will not be recorded in the database.
- **ListLocStatus** – Define the status for the instance that is found. The status will be recorded in the Compliance Guardian Online database.

  ***Note:** If the status set for **True result** or **False result** is **Fail**, the value for the **Status** attribute will be **Fail**, and the value cannot be changed.

- **CaseSensitive** – Define if the text being tested for must match the case exactly.
- **MustRepeat** – Define the amount of times a word or phrase must be found before considering the condition to be True.
- **CompareType** – Define **MustContain** or **MustEqual** for this attribute.
- **ResultNA** – If the primary check in this check is not fulfilled, the scan status will be the value you selected for the **ResultNA** attribute.

Secondary

Configure the following attributes in this section:

- **TrueIf** – Define the condition when the check result is True. If **Found** is specified: when finding an instance, the check result of this check will be True. If **NotFound** is specified: when finding an instance, the check result of this check will be False.
- **SearchAll** – Define whether or not to check the comments and scripts.
- **ListLoc** – Define whether or not to record the instance's location in the Compliance Guardian Online database. If **Yes** is specified, then every location of the instance found will be recorded in the Compliance Guardian Online database. If **No** is specified, the check continues, but the locations of the instances found will not be recorded in the database.
- **ListLocStatus** – Define the status for the instance that is found. The status will be recorded in the Compliance Guardian Online database.

  ***Note:** If the status set for **True result** or **False result** is **Fail**, the value for the **Status** attribute will be **Fail**, and the value cannot be changed.
- **CaseSensitive** – Define if the text being tested for must match the case exactly.
- **MustRepeat** – Define the amount of times a word or phrase must be found before considering the condition to be True.
- **CompareType** – Define **MustContain** or **MustEqual** for this attribute.
- **MaxDistanceToPrimary** – Specify the number of the characters. The scan engine extracts text as the scanning contents. In the contents, if the characters between a primary check instance (instance found in the primary check) and the secondary check instance (instance found in the secondary check) are less than the number specified here, the secondary check is Found.

RegEX

This test type will be represented by the Element <RegEx>. For example:

```
- <RegEx isFindText="Yes" CaseSensitive="Yes" MustRepoeat="1" ListLocStatus="Fail"
  SearchAll="Yes" ListLoc="Yes" TrueIf="NotFound">
      <![CDATA[\d{4}(-\d{5})?]]>
    - <Filter>
        <Text CaseSensitive="No" Separator=",">2147483647</Text>
        <Text CaseSensitive="No">2147483647</Text>
      - <Regex CaseSensitive="No">
          <![CDATA[\d{4}(-\d{5})?]]>
        </Regex>
      </Filter>
  </RegEx>
```

Figure 23: RegEx check.

RegEx

The **RegEx** section contains the following attributes:

- **IsFindText** – Define whether or not to extract the text as the scanning content. If **Yes** is specified, the scan engine will extract the text as the scanning content. if **No** is specified, the scan engine will use the source code as the scanning content.
- **SearchAll** – Define whether or not to check the comments and scripts.
- **CaseSensitive** – Define if the text being tested for must match the case exactly.
- **TrueIf** – Define the condition when the check result is True. If **Found** is specified: when finding an instance, the check result of this check will be True. If **NotFound** is specified: when finding an instance, the check result of this check will be False.
- **ListLoc** – Define whether or not to record the instance's location in the Compliance Guardian Online database. If **Yes** is specified, then every location of the instance found will be recorded in the Compliance Guardian Online database. If **No** is specified, the check continues, but the locations of the instances found will not be recorded in the database.
- **ListLocStatus** – Define the status for the instance that is found. The status will be recorded in the Compliance Guardian Online database.

  ***Note:** If the status set for **True result** or **False result** is **Fail**, the value for the **Status** attribute will be **Fail**, and the value cannot be changed.

- **MustRepeat** – Define the amount of times the value that matches the regular expression must be found before considering the condition to be True.
- **Value** – Specify a regular expression. The value that matches the regular expression will be scanned. The format of the regular expression must be **![CDATA[regular expression]]**.

Filter

The **Filter** section contains the following attributes:

- **CaseSensitive** – Define if the element being tested must match the case exactly.
- **Separator** – Define a separator if multiple values are specified.
- **Value** – Define one or more values for the test, and use the separator specified before to separate the values. If the scanned result that matches the specified regular expression exactly matches the value specified here, this result will be filtered out.
- The **Regex** section in **Filter** has the following attributes:
- **CaseSensitive** – Specify if the element being tested must match the case exactly.
- **Value** – Define a regular expression. If the scanned result that matches the specified regular expression also matches the regular expression specified here, this result will be

filtered out. The format of the regular expression must be **![CDATA[regular expression]]**.

ComplexRegEX

This test type will be represented by the Element <ComplexRegEx>. For example:

```
- <ComplexRegEx isFindText="Yes">
  - <Primary CaseSensitive="No" ListLocStatus="Note" ResultNA="NAResult" SearchAll="Yes"
    ListLoc="Yes" TrueIf="Found">
      <![CDATA[<text>]]>
    - <Filter>
        <Text CaseSensitive="No" Separator=",">2147483647</Text>
        <Text CaseSensitive="No">2147483647</Text>
      - <Regex CaseSensitive="No">
          <![CDATA[\d{4}(-\d{5})?]]>
        </Regex>
      </Filter>
    </Primary>
  - <Secondary CaseSensitive="No" ListLocStatus="Note" SearchAll="Yes" ListLoc="Yes"
    TrueIf="Found">
      <![CDATA[<Second>]]>
    - <Filter>
        <Text CaseSensitive="No" Separator=",">2147483647</Text>
        <Text CaseSensitive="No">2147483647</Text>
      - <Regex CaseSensitive="No">
          <![CDATA[\d{4}(-\d{5})?]]>
        </Regex>
      </Filter>
    </Secondary>
  </ComplexRegEx>
```

Figure 24: ComplexRegEX check.

ComplexRegex

The **ComplexRegex** section contains the following attribute:

- **IsFindText** – Define whether or not to extract the text as the scanning content. If **Yes** is defined, the scan engine will extract the text as the scanning content; if **No** is defined, the scan engine will use the source code as the scanning content.

Primary Check

The **Primary Check** section contains the following attributes:

- **SearchAll** – Define whether or not to check the comments and scripts.
- **CaseSensitive** – Define if the text being tested for must match the case exactly.
- **TrueIf** – Define the condition when the check result is True. If **Found** is defined: when finding an instance, the check result of this check will be True. If **NotFound** is defined: when finding an instance, the check result of this check will be False.
- **ListLoc** – Define whether or not to record the instance's location in the Compliance Guardian Online database. If **Yes** is defined, then every location of the instance found

will be recorded in the Compliance Guardian Online database. If **No** is defined, the check continues, but the locations of the instances found will not be recorded in the database.

- **ListLocStatus** – Define the status for the instance that is found. The status will be recorded in the Compliance Guardian Online database.

  ***Note:** If the status set for **True result** or **False result** is **Fail**, the value for the **Status** attribute will be **Fail**, and the value cannot be changed.

- **MustRepeat** – Define the amount of times the value that matches the regular expression must be found before considering the condition to be True.
- **ResultNA** – If the primary check in this check is not fulfilled, the scan status will be the value you selected for the **ResultNA** attribute.
- **Filter** – This field is optional. The **Filter** section has the following attributes:
  - **Text** – Configure the following attributes:
    - **CaseSensitive** – Define if the element being tested for must match the case exactly.
    - **Separator** – Define a separator if multiple values are specified.
    - **Value** – Define one or more values for the test, and use the separator specified before to separate the values. If the scanned result that matches the specified regular expression exactly matches the value specified here, this result will be filtered out.
  - **Regex** – Configure the following attributes:
    - **CaseSensitive** – Define if the element being tested for must match the case exactly.
    - **Separator** – Define a separator if multiple values are specified.
    - **Value** – Define a regular expression. If the scanned result that matches the specified regular expression also matches the regular expression specified here, this result will be filtered out. The format of the regular expression must be **![CDATA[regular expression]]**.

Secondary Check

The **Secondary Check** section contains the following attributes:

- **SearchAll** – Define whether or not to check the comments and scripts.
- **CaseSensitive** – Define if the text being tested for must match the case exactly.
- **TrueIf** – Define the condition when the check result is True. If **Found** is defined, when finding an instance, the check result of this check will be True. If **NotFound** is defined, when finding an instance, the check result of this check will be False.
- **ListLoc** – Define whether or not to record the instance's location in the Compliance Guardian Online database. If **Yes** is defined, then every location of the instance found

will be recorded in the Compliance Guardian Online database. If **No** is defined, the check continues, but the locations of the instances found will not be recorded in the database.

- **ListLocStatus** – Define the status for the instance that is found. The status will be recorded in the Compliance Guardian Online database.

  ***Note:** If the status set for **True result** or **False result** is **Fail**, the value for the **Status** attribute will be **Fail**, and the value cannot be changed.

- **MustRepeat** – Define the amount of times the value that matches the regular expression must be found before considering the condition to be True.
- **MaxDistanceToPrimary** – Specify the number of the characters. The scan engine extracts text as the scanning contents. In the contents, if the characters between a primary check instance (instance found in the primary check) and the secondary check instance (instance found in the secondary check) are less than the number specified here, the secondary check is Found.
- **Filter** – This is optional. The **Filter** section has the following attributes:
  - **Text** – Configure the following attributes:
    - **CaseSensitive** – Define if the element being tested for must match the case exactly.
    - **Separator** – Define a separator if multiple values are specified.
    - **Value** – Define one or more values for the test, and use the separator specified before to separate the values. If the scanned result that matches the specified regular expression exactly matches the value specified here, this result will be filtered out.
  - **Regex** – Configure the following attributes:
    - **CaseSensitive** – Define if the element being tested for must match the case exactly.
    - **Separator** – Define a separator if multiple values are specified.
    - **Value** – Define a regular expression. If the scanned result that matches the specified regular expression also matches the regular expression specified here, this result will be filtered out. The format of the regular expression must be **![CDATA[regular expression]]**.

Simple Element Validation

This test type will be represented by the Element <Element>. For example:

```
- <Element ValidWhen="true" TrueIf="All" ResultNA="NAResult" CaseSensitive="Yes" Name="img">
    <ListLoc Status="Warn" Type="Invalid"/>
    <ElementRepeat Alert="No">1000</ElementRepeat>
      <!-- Optional, outerHtml -->
    <TextCompare CaseSensitive="No" Separator="," CompareType="MustContain">x</TextCompare>
      <!-- Optional -->
  - <Attributes>
    - <Attribute CaseSensitive="Yes" Name="alt" MustExist="Yes" AllowNull="No">
        <Length CompareType="GreaterThan" Chars="5"/>
        <Length CompareType="LessThan" Chars="80"/>
        <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.img,.jpeg</TextCompare>
        <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.png</TextCompare>
        <WordsRepeat Number="4"/>
      </Attribute>
    </Attributes>
      <!-- Optional, InnerText -->
  - <ElementContent ContentReq="Yes">
      <Length CompareType="GreaterThan" Chars="0"/>
      <Length CompareType="LessThan" Chars="6"/>
      <TextCompare CaseSensitive="No" Separator="," CompareType="MustContain">x</TextCompare>
      <WordsRepeat Number="4"/>
    </ElementContent>
  + <ChildElement CaseSensitive="Yes" Name="d" MustExist="true">
  + <Filter>
  </Element>
```

Figure 25: Simple Element Validation check.

Element

The **Element** section contains the following attributes:

- **Name** – Define the element name that will be tested.
- **CaseSensitive** – Define if the element name being tested for must match the case exactly.
- **ResultNA** – Define the result when the specified element is not found. If **TrueResult** is defined, then if the specified element is not found, the True result will be returned. If **FalseResult** is selected, then if the specified element is not found, the False result will be returned. If **NAResult** is selected, then if the specified element is not found, the status of the tested file will be **Not Applicable**, which will be displayed in the Compliance Guardian Online report. In other words, you have the option to set the result to **Not Applicable** if none of the elements are found.
- **TrueIf** – There are two values for this attribute: **All** and **One**. If **One** is defined, the scan will stop when one instance is found (to save scan time). If **All** is defined, the scan will only stop when all instances are found.
- **ValidWhen** – This is used to indicate if the result is valid when the condition is one of two values: True or False.

ListLoc

The **ListLoc** section contains the following attributes:

- **Type** – There are two values for this attribute, **Valid** and **Invalid**. All elements that are considered valid or invalid are stored to the database (the Location).
- **Status** – This is used to indicate the disposition of the element and the severity selected by the user.

ElementRepeat

The **ElementRepeat** section contains the following attributes (this section is optional):

- **Alert** – Define whether to check for repeating elements.
- **Value** – Define the maximum times the element can repeat before the check is determined False.

TextCompare

The **TextCompare** section contains the following attributes (this section is optional):

- **CompareType** – Define the compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustEqual**, **MustMatch**, **MustNotMatch** and **MustNotEqual**.
- **Separator** – Define a separator if multiple values are specified.
- **CaseSensitive** – Define if the element being tested for must match the case exactly.

Attributes

The **Attributes** section contains the following attributes (this section is optional):

- **Name** – Define attribute name that will be tested.
- **CaseSensitive** – Define if the attribute name being tested for must match the case exactly.
- **AllowNull** – Define whether the attribute that has no value will be tested.
- **MustExist** – Define whether or not the attribute has to exist. If it is set to **True**, then the test will fail if the specified attribute does not exist.

The following elements with specific attributes appear within the optional **Attributes** section:

- **Length** – This element is optional:
    - **CompareType** – Define a compare type for this length compare. The attributes for CompareType are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal**, and **NotEqual**.
    - **Characters** – Define the number of the characters used for the compare.

- **TextCompare** – This element is optional:
    - **CompareType** – Define a compare type. The attributes for CompareType are MustContain, MustNotContain, MustEqual, MustMatch, MustNotMatch and MustNotEqual.
    - **Separator** – Define a separator if multiple values are specified.
    - **CaseSensitive** – Define if the attribute values being tested for must match the case exactly.
- **WordsRepeat** – This element is optional:
    - **Number** – Define the number of times that words can repeat in the attribute value. If the number of times that words are repeating is greater than or equal to the defined value, the test will fail.

ElementContent

The section contains the following attributes (this section is optional):

- **ContentReq** – Define whether the specified element must contain content. If **Yes** is defined, then the element must contain content, or the check for this section will be False.

The following elements with specific attributes are within the optional **ElementContent** section:

- **Length** – This section is optional:
    - **CompareType** – Define a compare type for this length compare. The attributes for CompareType are GreaterThan, LessThan, GreaterOrEqualThan, LessOrEqualThan, Equal and NotEqual.
    - **Characters** – Define the number of the characters used for the compare.
- **TextCompare** – This section is optional. Select the checkbox before this element, the following attributes appear:
    - **CompareType** – Define a compare type. The attributes for CompareType are MustContain, MustNotContain, MustEqual, MustMatch, MustNotMatch and MustNotEqual.
    - **Separator** – Define a separator if multiple values are specified.
    - **CaseSensitive** – Define if the content being tested for must match the case exactly.
- **WordsRepeat** – This element is optional:
    - **Number** – Define the number of times that words can repeat. If the number of times that words are repeating is greater than or equal to the defined value, the test will fail.

ChildElement

The **ChildElement** section contains the following attributes (this section is optional):

- **Name** – Define the name of the child element that will be tested.
- **CaseSensitive** – Define if the element name being tested for must match the case exactly.
- **MustExist** – Define whether or not the child element must exist. If **True** is defined, then the test will fail if there is No child element.

The following elements with specific attributes are within the optional **ChildElement** section:

- **ElementRepeat** – This section is optional:
  - **Alert** – Define whether to check for repeating elements.
- **Attributes** – This section is optional:
  - **Name** – Define the attribute name that will be tested.
  - **CaseSensitive** – Define if the attribute name being tested for must match the case exactly.
  - **AllowNull** – Define whether the attribute that has no value will be tested.
  - **MustExist** – Define whether or not the attribute has to exist. If True is selected, then the test will fail if the specified attribute does not exist.

  The following elements with specific attributes are within the optional **Attributes** section:

  - **Length** – This section is optional:
    - **CompareType** – Define a compare type for this length compare. The attributes for **CompareType** are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal** and **NotEqual**.
    - **Characters** – Define the number of the characters used for the compare.
  - **TextCompare** – This section is optional:
    - **CompareType** – Define a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustMatch**, **MustNotMatch**, **MustEqual**, and **MustNotEqual**.
    - **Separator** – Define a separator if multiple values are specified.
    - **CaseSensitive** – Define if the attribute being tested for must match the case exactly.
  - **WordsRepeat** – This section is optional:
    - **Number** – Define the number of times that words can repeat in the attribute value before the test fails. If the number of times that words

are repeating is greater than or equal to the defined value, the test will fail.

- **ElementContent** – This section is optional:
  - **ContentReq** – Define whether the specified element must contain content. If **Yes** is defined, then the element must contain content, or the check for this section will be False.

  The following elements with specific attributes are within the optional **ElementContent** section:

  - **Length** – This section is optional:
    - **CompareType** – Define a compare type for this length compare. The attributes for CompareType are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal,** and **NotEqual**.
    - **Characters** – Define the number of the characters used for the compare.
  - **TextCompare** – This section is optional:
    - **CompareType** – Define a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustMatch**, **MustNotMatch**, **MustEqual**, and **MustNotEqual**.
    - **Separator** – Define a separator if multiple values are specified.
    - **CaseSensitive** – Define if the attribute being tested for must match the case exactly.

FindFile

This test type will be represented by the Element <FindFile>. For example:

```
<FindFile TureIf="found">p3c.txt</FindFile>
```

Figure 26: FindFile check.

The **FindFile** section contains the following attributes:

- **TrueIf** – Define the condition when the check result is **True**. If **Found** is defined, when finding an instance, the check result of this check will be True; If **NotFound** is defined: when finding an instance, the check result of this check will be False.
- **Path** – Enter the file's relative path or full path beside the value of **TrueIf**.

Web Beacon

This test type will be represented by the <Beacons>. For example:

```
</DomainExclude>When="True" AttrCaseSensitive="Yes" AttrName="src" ResultNA="NAResult" Sensitive="Yes"
  ElementName="img">
    - <Elements WhereDomain="External" Scope="All">
        <ListLoc Status="Warn" Type="Invalid"/>
        <DomainExclude>http://www.baidu.com/</DomainExclude>
      </Elements>
  </Beacons>
```

Figure 27: Web Beacon check.

Beacons

The **Beacons** section contains the following attributes:

- **ElementName** – Define the element name that will be tested.
- **CaseSensitive** – Define if the element name being tested for must match the case exactly.
- **ResultNA** – Define a result when the specified element is not found. If **TrueResult** is defined, then if the specified element is not found, the True result will be returned; if **FalseResult** is defined, then if the specified element is not found, the False result will be returned; if **NAResult** is defined, then if the specified element is not found, the status of the tested file will be **Not Applicable**, which will be displayed in the Compliance Guardian Online report. This is basically stating that you have the option to set the result to **Not Applicable** if none of the elements are found.
- **AttrName** – Define the attribute name that will be tested.
- **AttrCaseSensitive** – Define if the attribute name being tested for must match the case exactly.
- **ValidWhen** – This is used to indicate if the result is valid when the condition is one of two values: True or False.

Elements

The **Elements** section contains the following attribute:

- **Scope** – There are two values for this attribute: **All** and **One**. If **One** is defined, the scan will stop when one instance is found (to save scan time). If **All** is defined, the scan will only stop when all instances are found.

ListLoc

The **ListLoc** section contains the following attributes:

- **Type** – There are two values for this attribute, **Valid** and **Invalid**. All elements that are considered valid or invalid are stored to the database (the Location).

- **Status** – This is used to indicate the disposition of the element and the severity selected by the user.

  ***Note:** If the status set for **True result** or **False result** is **Fail**, the value for the **Status** attribute will be **Fail**, and the value cannot be changed.

DomainExclude

The **DomainExclude** section contains the following attributes:

- **Separator** – You can add this attribute when you edit the check. This is used to specify a separator if multiple values are specified.
- **Value** – Define one or more domains here, the links that are located in these domains will not be checked. Use the separator specified before to separate the values.

SSL (Validation)

This test type will be represented by the Element <SSLValidation>. For example:

```
- <SSLValidation MinLevel="64" AttrCaseSensitive="No" AttrName="value" ResultNA="NAResult"
  CaseSensitive="Yes" ElementName="input">
      <TextCompare CaseSensitive="No" Separator="," CompareType="MustContain">First</TextCompare>
      <TextCompare CaseSensitive="No" Separator="," CompareType="MustContain">last</TextCompare>
      <TextCompare CaseSensitive="No" Separator="," CompareType="MustContain">City</TextCompare>
  </SSLValidation>
```

Figure 28: SSL check.

SSL

The **SSL** section contains the following attributes:

- **ElementName** – This is the element that will be tested.
- **CaseSensitive** – Instruct the testing core if the element name being tested for must match the case exactly.
- **ResultNA** – Define a result when the specified element is not found. If **TrueResult** is defined, then if the specified element is not found, the True result will be returned. If **FalseResult** is defined, then if the specified element is not found, the False result will be returned; if **NAResult** is defined, then if the specified element is not found, the status of the tested file will be **Not Applicable**, which will be displayed in the Compliance Guardian Online report. In other words, you have the option to set the result to **Not Applicable** if none of the elements are found.
- **AttrName** – This is the attribute that will be tested.
- **AttrCaseSensitive** – Instruct the testing core if the attribute name being tested for must match the case exactly.
- **MinLevel** – Represent the minimum HTTPS protocol encryption level required by the check.

TextCompare

This **TextCompare** section is optional. The section contains the following attributes:

- **CompareType** – Define a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustEqual**, **MustMatch**, **MustNotMatch** and **MustNotEqual**.
- **Separator** – Define a separator if multiple values are specified.
- **CaseSensitive** – Define if the attribute being tested for must match the case exactly.
- **Value** – Define one or more values for the test, use the separator specified before to separate the values.

Cookie (Validation)

This test type will be represented by the Element <CookieValidation>. For example:

```
<CookieValidation cPIITdf="1" Expires="100000" ResultNA="NAResult" PrivacyLink="bbc.com"
    PrivacyLinkReq="True" ThirdParty="true" cType="1"> </CookieValidation>
```

Figure 29: Cookie check.

The **Cookie (Validation)** section contains the following attributes:

- **ThirdParty** – Instruct the scan engine to check if the cookie is from a third party.
- **PrivacyLinReq** – Instruct the scan engine (based on the cookie condition) to check for a privacy link.
- **ResultNA** – Define a result when the specified element is not found. If **TrueResult** is defined, then if the specified element is not found, the True result will be returned; if **FalseResult** is defined, then if the specified element is not found, the False result will be returned. If **NAResult** is defined, then if the specified element is not found, the status of the tested file will be **Not Applicable**, which will be displayed in the Compliance Guardian Online report. This is basically stating that you have the option to set the result to **Not Applicable** if none of the elements are found.
- **Expires** – Instruct the testing core to check when the cookie expires in N seconds.
- **cPIITDF** – Instruct the testing core to use the specified check to identify PII in the webpage.
- **CType** – Identify the cookie type to test for (allowed values 1, 2, 3):
    - **1** – Single session. This tier encompasses any use of single session Web measurement and customization technologies.
    - **2** – Multi-session without PII. This tier encompasses any use of multi-session Web measurement and customization technologies when no PII is collected (including when the agency is unable to identify an individual as a result of its use of those technologies).

- **3** – Multi-session with PII. This tier encompasses any use of multi-session Web measurement and customization technologies when PII is collected (including when the agency is able to identify an individual as a result of its use of those technologies).

- **PrivacyLink** – If the privacy link in the file contains the value specified here, this check will be True.

Dictionary

This test type will be represented by the Element <FindTextGroup>. For example:

```
- <FindTextGroup BreakIfFound="True">
  - <FindText CompareType="MustEqual" CaseSensitive="No" ListLocStatus="Warn" SearchAll="Yes" ListLoc="Yes"
    TrueIf="NotFound">
      <Dictionary Separator=",">text1,text2 , text3</Dictionary>
    </FindText>
  - <Regex CaseSensitive="No" ListLocStatus="Fail" SearchAll="Yes" ListLoc="Yes" TrueIf="NotFound">
      <Dictionary Separator=",">text(4|5), text1?1</Dictionary>
    - <Filter>
        <Text CaseSensitive="No" Separator=",">2147483647</Text>
        <Text CaseSensitive="No">2147483647</Text>
      - <Regex CaseSensitive="No">
          <![CDATA[\d{4}(-\d{5})?]]>
        </Regex>
      </Filter>
    </Regex>
</FindTextGroup>
```

Figure 30: Dictionary check.

Dictionary

The **Dictionary** section contains the following attribute:

- **BreakIfFound** – Define **Yes** or **No** for this attribute. If **Yes** is defined, the scan will stop when one instance is found (to save scan time). If **No** is defined, the scan will only stop when all instances are found.

FindText

This **FindText** section is optional. The section contains the following attributes:

- **FindText** – The section contains the following attributes:
  - **TrueIf** – Define the condition when the check result is True. If **Found** is defined, when finding an instance, the check result of this check will be True. If **NotFound** is defined, when finding an instance, the check result of this check will be False.
  - **SearchAll** – Define whether or not to check the comments and scripts.
  - **ListLoc** – Define whether or not to record the instance's location in the Compliance Guardian Online database. If **Yes** is defined, then every location of the instance found will be recorded in the Compliance Guardian Online

database. If **No** defined, the check continues, but the locations of the instances found will not be recorded in the database.

- **ListLocStatus** – Define the status for the instance that is found. The status will be recorded in the Compliance Guardian Online database.

  ***Note:** If the status set for **True result** or **False result** is **Fail**, the value for the **Status** attribute will be **Fail**, and the value cannot be changed.

- **CaseSensitive** – Define if the text being tested for must match the case exactly.
- **CompareType** – Define **MustContain** or **MustEqual** for this attribute.

- **Dictionary** – The section contains the following attributes:
  - **Separator** – Define a separator if multiple values are specified.
  - **Value** – Define one or more values for the test, use the separator specified before to separate the values.

Regex

This **Regex** section is optional. The section contains the following attributes:

- The **Regex** section contains the following attributes:
  - **TrueIf** – Define the condition when the check result is True. If **Found** is defined, when finding an instance, the check result of this check will be True. If **NotFoun**d is defined, when finding an instance, the check result of this check will be False.
  - **SearchAll** – Define whether or not to check the comments and scripts.
  - **ListLoc** – Define whether or not to record the instance's location in the Compliance Guardian Online database. If **Yes** is defined, then every location of the instance found will be recorded in the Compliance Guardian Online database. If **No** is defined, the check continues, but the locations of the instances found will not be recorded in the database.
  - **ListLocStatus** – Define the status for the instance that is found. The status will be recorded in the Compliance Guardian Online database. Note that if the status set for **True result** or **False result** is **Fail**, the value for the **Status** attribute will be **Fail**, and the value cannot be changed.
  - **CaseSensitive** – Define if the text being tested for must match the case exactly.
- **Dictionary** – Configure the following attributes:
  - **Separator** – Define a separator if multiple values are specified.
  - **Value** – Define one or more values for the test, use the separator specified before to separate the values.

- **Filter** – The **Regex** section contains the following attributes:
    - **Text** – Configure the following attributes:
        - **CaseSensitive** – Define if the element being tested for must match the case exactly.
        - **Separator** – Define a separator if multiple values are specified.
        - **Value** – Define one or more values for the test, and use the separator specified before to separate the values. If the scanned result that matches the specified regular expression exactly matches the value specified here, this result will be filtered out.
    - **Regex** – Configure the following attributes:
        - **CaseSensitive** – Define if the element being tested for must match the case exactly.
        - **Separator** – Define a separator if multiple values are specified.
        - **Value** – Define a regular expression. If the scanned result that matches the specified regular expression also matches the regular expression specified here, this result will be filtered out. The format of the regular expression must be **![CDATA[regular expression]]**.

Enhanced Element

This test type will be represented by the Element <EnhancedElement>. For example:

```
- <EnhancedElement ValidWhen="true" TrueIf="All" ResultNA="NAResult" CaseSensitive="No" Name="map">
    <ListLoc Status="Warn" Type="Invalid"/>
      <!-- Optional -->
    <ElementRepeat Alert="No">1000</ElementRepeat>
      <!-- Optional -->
    <TextCompare CaseSensitive="No" Separator="," CompareType="MustContain">x</TextCompare>
      <!-- Optional -->
  - <Attributes>
        <!--Optional one to many -->
    - <Attribute CaseSensitive="Yes" Name="LongDesc" MustExist="Yes" AllowNull="No">
        <Length CompareType="GreaterThan" Chars="0"/>
        <Length CompareType="LessThan" Chars="80"/>
        <TextCompare CaseSensitive="Yes" Separator="," CompareType="MustContain">test</TextCompare>
        <WordsRepeat Number="1"/>
      </Attribute>
    </Attributes>
      <!--Optional -->
  + <ElementContent ContentReq="Yes">
      <!--Optional -->
  + <ChildElement CaseSensitive="Yes" Name="d" MustExist="true">
      <!--Optional -->
  - <SecondaryElement TrueIf="First" CaseSensitive="Yes" Name="a" MustExist="Yes" MustNext="true">
        <!-- Optional -->
      <ElementRepeat Alert="No">1000</ElementRepeat>
        <!--Optional -->
    + <Attributes>
        <!--Optional -->
    + <ElementContent ContentReq="Yes">
        <!--Optional -->
    + <ChildElement CaseSensitive="Yes" Name="d" MustExist="true" UseElementContentTest="Yes" UseAttrTest="Yes">
    </SecondaryElement>
      <!-- Optional -->
  + <Filter>
  </EnhancedElement>
```

Figure 31: Enhanced Element check.

EnhancedElement

The E**nhancedElement** section contains the following attributes:

- **Name** – Define the element name that will be tested.
- **CaseSensitive** – Define if the element name being tested for must match the case exactly.
- **ResultNA** – Define the result when the specified element is not found. If **TrueResult** is defined, then if the specified element is not found, the True result will be returned. If **FalseResult** is selected, then if the specified element is not found, the False result will be returned. If **NAResult** is selected, then if the specified element is not found, the status of the tested file will be **Not Applicable**, which will be displayed in the Compliance Guardian Online report. In other words, you have the option to set the result to **Not Applicable** if none of the elements are found.
- **TrueIf** – There are two values for this attribute: **All** and **One**. If **One** is defined, the scan will stop when one instance is found (to save scan time). If **All** is defined, the scan will only stop when all instances are found.
- **ValidWhen** – This is used to indicate if the result is valid when the condition is one of two values: True or False.

ListLoc

The **ListLoc** section contains the following attributes:

- **Type** – There are two values for this attribute, **Valid** and **Invalid**. All elements that are considered valid or invalid are stored to the database (the Location).
- **Status** – This is used to indicate the disposition of the element and the severity selected by the user.

ElementRepeat

The **ElementRepeat** section contains the following attributes (this section is optional):

- **Alert** – Define whether to check for repeating elements.
- **Value** – Define the maximum times the element can repeat before the check is determined False.

TextCompare

The **TextCompare** section contains the following attributes (this section is optional):

- **CompareType** – Define the compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustEqual**, **MustMatch**, **MustNotMatch** and **MustNotEqual**.
- **Separator** – Define a separator if multiple values are specified.

- **CaseSensitive** – Define if the element being tested for must match the case exactly.

Attributes

The **Attributes** section contains the following attributes (this section is optional):

- **Name** – Define attribute name that will be tested.
- **CaseSensitive** – Define if the attribute name being tested for must match the case exactly.
- **AllowNull** – Define whether the attribute that has no value will be tested.
- **MustExist** – Define whether or not the attribute has to exist. If it is set to **True**, then the test will fail if the specified attribute does not exist.

The following elements with specific attributes appear within the optional **Attributes** section:

- **Length** – This element is optional:
  - **CompareType** – Define a compare type for this length compare. The attributes for CompareType are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal**, and **NotEqual**.
  - **Characters** – Define the number of the characters used for the compare.
- **TextCompare** – This element is optional:
  - **CompareType** – Define a compare type. The attributes for CompareType are MustContain, MustNotContain, MustEqual, MustMatch, MustNotMatch and MustNotEqual.
  - **Separator** – Define a separator if multiple values are specified.
  - **CaseSensitive** – Define if the attribute values being tested for must match the case exactly.
- **WordsRepeat** – This element is optional:
  - **Number** – Define the number of times that words can repeat in the attribute value before the test fails. If the number of times that words are repeating is greater than or equal to the defined value, the test will fail.

ElementContent

The **ElementContent** section contains the following attributes (this section is optional):

- **ContentReq** – Define whether the specified element must contain content. If **Yes** is defined, then the element must contain content, or the check for this section will be False.

The following elements with specific attributes are within the optional **ElementContent** section:

- **Length** – This section is optional:
  - **CompareType** – Define a compare type for this length compare. The attributes for CompareType are GreaterThan, LessThan, GreaterOrEqualThan, LessOrEqualThan, Equal and NotEqual.
  - **Characters** – Define the number of the characters used for the compare.
- **TextCompare** – This section is optional. Select the checkbox before this element, the following attributes appear:
  - **CompareType** – Define a compare type. The attributes for CompareType are MustContain, MustNotContain, MustEqual, MustMatch, MustNotMatch and MustNotEqual.
  - **Separator** – Define a separator if multiple values are specified.
  - **CaseSensitive** – Define if the content being tested for must match the case exactly.

ChildElement

The **ChildElement** section contains the following attributes (this section is optional):

- **Name** – Define the name of the child element that will be tested.
- **CaseSensitive** – Define if the element name being tested for must match the case exactly.
- **MustExist** – Define whether or not the child element must exist. If **True** is defined, then the test will fail if there is No child element.

The following elements with specific attributes are within the optional **ChildElement** section:

- **ElementRepeat** – This section is optional:
  - **Alert** – Define whether to check for repeating elements.
- **Attributes** – This section is optional:
  - **Name** – Define the attribute name that will be tested.
  - **CaseSensitive** – Define if the attribute name being tested for must match the case exactly.
  - **AllowNull** – Define whether the attribute that has no value will be tested.
  - **MustExist** – Define whether or not the attribute has to exist. If True is selected, then the test will fail if the specified attribute does not exist.

The following elements with specific attributes are within the optional **Attributes** section:

- **Length** – This section is optional:
  - **CompareType** – Define a compare type for this length compare. The attributes for **CompareType** are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal** and **NotEqual**.
  - **Characters** – Define the number of the characters used for the compare.
- **TextCompare** – This section is optional:
  - **CompareType** – Define a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustMatch**, **MustNotMatch**, **MustEqual**, and **MustNotEqual**.
  - **Separator** – Define a separator if multiple values are specified.
  - **CaseSensitive** – Define if the attribute being tested for must match the case exactly.
- **WordsRepeat** – This section is optional:
  - **Number** – Define the number of times that words can repeat in the attribute value before the test fails. If the number of times that words are repeating is greater than or equal to the defined value, the test will fail.
- **ElementContent** – This section is optional:
  - **ContentReq** – Define whether the specified element must contain content. If **Yes** is defined, then the element must contain content, or the check for this section will be False.

  The following elements with specific attributes are within the optional **ElementContent** section:

  - **Length** – This section is optional:
    - **CompareType** – Define a compare type for this length compare. The attributes for CompareType are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal,** and **NotEqual**.
    - **Characters** – Define the number of the characters used for the compare.
  - **TextCompare** – This section is optional:
    - **CompareType** – Define a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustMatch**, **MustNotMatch**, **MustEqual**, and **MustNotEqual**.
    - **Separator** – Define a separator if multiple values are specified.

- **CaseSensitive** – Define if the attribute being tested for must match the case exactly.

SecondaryElement

This **SecondaryElement** section is optional. The section contains the following attributes:

- **Name** – Define the secondary element that will be tested.
- **CaseSensitive** – Define if the element name being tested for must match the case exactly.
- **MustExist** – Define whether the secondary element must exist.
- **TrueIf** – There are two values for this attribute: **All** and **One**. If **One** is selected, the scan will stop when one instance is found (to save scan time). If **All** is selected, the scan will only stop when all instances are found.
- **MustNext** – Define whether the secondary element must be next to the primary element (the element you specified above in this check). If **Yes** is defined, only the secondary element that is next to the primary element will be checked. If **No** is defined, then all the specified secondary elements will be checked.

The following elements with specific attributes are within the optional **SecondaryElement** section:

- **ElementRepeat** – This section is optional:
  - **Alert** – Define whether to check for repeating elements.
  - **Value** – Define the maximum times the element can repeat before the check is determined False.
- **Attributes** – This section is optional:
  - **Name** – Define the attribute name that will be tested.
  - **CaseSensitive** – Define if the attribute name being tested for must match the case exactly.
  - **AllowNull** – Define whether the attribute that has no value will be tested.
  - **MustExist** – Define whether or not the attribute has to exist. If True is selected, then the test will fail if the specified attribute does not exist.

  The following elements with specific attributes are within the optional **Attributes** section:

  - **Length** – This section is optional:
    - **CompareType** – Define a compare type for this length compare. The attributes for **CompareType** are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal**, and **NotEqual**.
    - **Characters** – Define the number of the characters used for the compare.

- **TextCompare** – This section is optional:
  - **CompareType** – Define a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustMatch**, **MustNotMatch**, **MustEqual**, and **MustNotEqual**.
  - **Separator** – Define a separator if multiple values are specified.
  - **CaseSensitive** – Define if the attribute being tested for must match the case exactly.
  - **Value** – Define one or more values for the test, use the Separator specified before to separate the values.
- **WordsRepeat** – This section is optional.
  - **Number** – Define the number of times that words can repeat in the attribute value before the test fails. If the number of times that words are repeating is greater than or equal to the defined value, the test will fail.

- **ElementContent** – This section is optional:
  - **ContentReq** – Define whether the specified element must contain content. If **Yes** is selected, then the element must contain content, or the check for this section will be False.

  The following elements with specific attributes are within the optional **ElementContent** section:

  - **Length** – This section is optional:
    - **CompareType** – Define a compare type for this length compare. The attributes for CompareType are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal**, and **NotEqual**.
    - **Characters** – Define the number of the characters used for the compare.
  - **TextCompare** – This **section** is optional:
    - **CompareType** – Define a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustMatch**, **MustNotMatch**, **MustEqual**, and **MustNotEqual**.
    - **Separator** – Define a separator if multiple values are specified.
    - **CaseSensitive** – Define if the attribute being tested for must match the case exactly.
    - **Value** – Define one or more values for the test, use the separator specified before to separate the values.
- **ChildElement** – This section is optional:
  - **Name** – Define the name of the child element that will be tested.

- **CaseSensitive** – Define whether the element name being tested for must match the case exactly.
- **MustExist** – Define whether or not the child element must exist. If True is selected, then the test will fail if there is No child element.

The following elements with specific attributes are within the optional **ChildElement** section:

- **ElementRepeat** – This section is optional:
  - **Alert** – Define whether to check for repeating elements.
  - **Value** – Define the maximum times the element can repeat before the check is determined False.
- **Attributes** – This section is optional:
  - **Name** – Define the attribute name that will be tested.
  - **CaseSensitive** – Define if the attribute name being tested for must match the case exactly.
  - **AllowNull** – Define whether the attribute that has no value will be tested.
  - **MustExist** – Define whether or not the attribute has to exist. If True is selected, then the test will fail if the specified attribute does not exist.

  The following elements with specific attributes are within the optional **Attributes** section:

- **Length** – This section is optional:
  - **CompareType** – Define a compare type for this length compare. The attributes for CompareType are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal**, and **NotEqual**.
  - **Characters** – Define the number of the characters used for the compare.

Match Element Validation

This test type will be represented by the Element <MatchElement>. For example:

```
- <MatchElement ValidWhen="True" TrueIf="All" ResultNA="NAResult" CaseSensitive="Yes" Name="Input">
    <ListLoc Status="Fail" Type="Invalid"/>
      <!-- Optional -->
  - <Attributes>
    - <Attribute CaseSensitive="Yes" Name="id" MustExist="Yes" AllowNull="No">
        <Length Chars="0" CompareType="GreaterThan"/>
        <Length Chars="20" CompareType="LessThan"/>
        <TextCompare CaseSensitive="No" CompareType="MustNotContain" Separator=",">.pdf</TextCompare>
        <WordsRepeat Number="6"/>
      </Attribute>
    </Attributes>
      <!-- Optional -->
  - <ElementContent ContentReq="false">
      <Length Chars="0" CompareType="GreaterThan"/>
      <Length Chars="20" CompareType="LessThan"/>
      <TextCompare CaseSensitive="No" CompareType="MustContain" Separator=","/>
    </ElementContent>
      <!-- Optional -->
    <ChildElement CaseSensitive="Yes" Name="d" MustExist="true"/>
  - <SecondaryMatch ValidWhen="True" TrueIf="All" ResultNA="NAResult" CaseSensitive="Yes" Name="label">
    - <Attribute CaseSensitive="Yes" Name="For" MustExist="true" AllowNull="No">
      - <TextCompare>
          <MatchAttributeValue CaseSensitive="No" Name="id" CompareType="MustContain"/>
            <!--<MatchElementContent CompareType="MustNotContain" CaseSensitive="No" />-->
          <TextCompare CaseSensitive="No" CompareType="MustContain"
            Separator=",">http://www.google.com</TextCompare>
        </TextCompare>
      </Attribute>
    </SecondaryMatch>
</MatchElement>
```

Figure 32: Match Element Validation check.

MatchElement

The **MatchElement** section contains the following attributes:

- **Name** – Define the element name that will be tested.
- **CaseSensitive** – Define if the element name being tested for must match the case exactly.
- **ResultNA** – Define the result when the specified element is not found. If **TrueResult** is defined, then if the specified element is not found, the True result will be returned. If **FalseResult** is selected, then if the specified element is not found, the False result will be returned. If **NAResult** is selected, then if the specified element is not found, the status of the tested file will be **Not Applicable**, which will be displayed in the Compliance Guardian Online report. In other words, you have the option to set the result to **Not Applicable** if none of the elements are found.
- **TrueIf** – There are two values for this attribute: **All** and **One**. If **One** is defined, the scan will stop when one instance is found (to save scan time). If **All** is defined, the scan will only stop when all instances are found.
- **ValidWhen** – This is used to indicate if the result is valid when the condition is one of two values: True or False.

ListLoc

The **ListLoc** section contains the following attributes:

- **Type** – There are two values for this attribute, **Valid** and **Invalid**. All elements that are considered valid or invalid are stored to the database (the Location).
- **Status** – This is used to indicate the disposition of the element and the severity selected by the user.

Attributes

The **Attributes** section contains the following attributes (this section is optional):

- **Name** – Define attribute name that will be tested.
- **CaseSensitive** – Define if the attribute name being tested for must match the case exactly.
- **AllowNull** – Define whether the attribute that has no value will be tested.
- **MustExist** – Define whether or not the attribute has to exist. If it is set to **True**, then the test will fail if the specified attribute does not exist.

The following elements with specific attributes appear within the optional **Attributes** section:

- **Length** – This element is optional:
  - **CompareType** – Define a compare type for this length compare. The attributes for CompareType are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal**, and **NotEqual**.
  - **Characters** – Define the number of the characters used for the compare.
- **TextCompare** – This element is optional:
  - **CompareType** – Define a compare type. The attributes for CompareType are MustContain, MustNotContain, MustMatch, MustNotMatch, MustEqual, and MustNotEqual.
  - **Separator** – Define a separator if multiple values are specified.
  - **CaseSensitive** – Define if the attribute values being tested for must match the case exactly.
- **WordsRepeat** – This element is optional:
  - **Number** – Define the number of times that words can repeat in the attribute value before the test fails. If the number of times that words are repeating is greater than or equal to the defined value, the test will fail.

ElementContent

The **ElementContent** section contains the following attributes (this section is optional):

- **ContentReq** – Define whether the specified element must contain content. If **Yes** is defined, then the element must contain content, or the check for this section will be False.

The following elements with specific attributes are within the optional **ElementContent** section:

- **Length** – This section is optional:
  - **CompareType** – Define a compare type for this length compare. The attributes for CompareType are GreaterThan, LessThan, GreaterOrEqualThan, LessOrEqualThan, Equal and NotEqual.
  - **Characters** – Define the number of the characters used for the compare.
- **TextCompare** – This section is optional. Select the checkbox before this element, the following attributes appear:
  - **CompareType** – Define a compare type. The attributes for CompareType are MustContain, MustNotContain, MustMatch, MustNotMatch, MustEqual and MustNotEqual.
  - **Separator** – Define a separator if multiple values are specified.
  - **CaseSensitive** – Define if the content being tested for must match the case exactly.

ChildElement

The **ChildElement** section contains the following attributes (this section is optional):

- **Name** – Define the name of the child element that will be tested.
- **CaseSensitive** – Define if the element name being tested for must match the case exactly.
- **MustExist** – Define whether or not the child element must exist. If **True** is defined, then the test will fail if there is No child element.

The following elements with specific attributes are within the optional **ChildElement** section:

- **ElementRepeat** – This section is optional:
  - **Alert** – Define whether to check for repeating elements.
- **Attributes** – This section is optional:
  - **Name** – Define the attribute name that will be tested.
  - **CaseSensitive** – Define if the attribute name being tested for must match the case exactly.
  - **AllowNull** – Define whether the attribute that has no value will be tested.

- **MustExist** – Define whether or not the attribute has to exist. If True is selected, then the test will fail if the specified attribute does not exist.

The following elements with specific attributes are within the optional **Attributes** section:

- **Length** – This section is optional:
  - **CompareType** – Define a compare type for this length compare. The attributes for **CompareType** are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal** and **NotEqual**.
  - **Characters** – Define the number of the characters used for the compare.
- **TextCompare** – This section is optional:
  - **CompareType** – Define a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustMatch**, **MustNotMatch**, **MustEqual**, and **MustNotEqual**.
  - **Separator** – Define a separator if multiple values are specified.
  - **CaseSensitive** – Define if the attribute being tested for must match the case exactly.
- **WordsRepeat** – This section is optional:
  - **Number** – Define the number of times that words can repeat in the attribute value before the test fails. If the number of times that words are repeating is greater than or equal to the defined value, the test will fail.
- **ElementContent** – This section is optional:
  - **ContentReq** – Define whether the specified element must contain content. If **Yes** is defined, then the element must contain content, or the check for this section will be False.

  The following elements with specific attributes are within the optional **ElementContent** section:

  - **Length** – This section is optional:
    - **CompareType** – Define a compare type for this length compare. The attributes for CompareType are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal,** and **NotEqual**.
    - **Characters** – Define the number of the characters used for the compare.
  - **TextCompare** – This section is optional:
    - **CompareType** – Define a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustMatch**, **MustNotMatch**, **MustEqual**, and **MustNotEqual**.

- **Separator** – Define a separator if multiple values are specified.
- **CaseSensitive** – Define if the attribute being tested for must match the case exactly.

SecondaryMatch

This **SecondaryMatch** section is optional. The section contains the following attributes:

- **SecondaryMatch** – The element has the following attributes:
  - **Name** – Define the element that will be tested.
  - **CaseSensitive** – Define if the element name being tested for must match the case exactly.
  - **ResultNA** – Define a result when the specified element is not found. If **TrueResult** is defined, then if the specified element is not found, the True result will be returned. If **FalseResult** is defined, then if the specified element is not found, the False result will be returned. If **NAResult** is defined, then if the specified element is not found, the status of the tested file will be **Not Applicable**, which will be displayed in the Compliance Guardian Online report. This is basically stating that you have the option to set the result to **Not Applicable** if none of the elements are found.
  - **TrueIf** – There are two values for this attribute: **All** and **One**. If **One** is defined, the scan will stop when one instance is found (to save scan time). If **All** is defined, the scan will only stop when all instances are found.
  - **ValidWhen** – This is used to indicate if the result is valid when the condition is one of two values: True or False.
- **Attribute** – The element has the following attributes:
  - **Name** – Define the name of the attribute to be tested.
  - **CaseSensitive** – Define if the attribute name being tested for must match the case exactly.
  - **AllowNull** – Define whether the attribute that has no value will be tested.
  - **MustExist** – Define whether or not the attribute has to exist. If **True** is selected, then the test will fail if the specified attribute does not exist.
- **TextCompare** – The element has the following attributes:
  - **MatchElementValue** – Configure the following attributes:
    - **Name** – Define a name for the test.
    - **CaseSensitive** – Define if the attribute name being tested for must match the case exactly.
    - **CompareType** – There are two values for this attribute: **MustContain** and **MustNotContain**. If **MustContain** is defined, the test condition is: the value of the attribute under the **SecondaryMatch** section must

contain the value of the attribute under the **MatchElement** section, or the check will be failed; If **MustNotContain** is defined, the test condition is: the value of the attribute under the **SecondaryMatch** section must not contain the value of the attribute under the **MatchElement** section, or the check will be failed.

- **TextCompare** – The element has the following attributes:
  - **CompareType** – Define a compare type. The attributes for **CompareType** are **MustContain**, **MustMatch**, **MustNotMatch**, **MustNotContain**, **MustEqual**, and **MustNotEqual**.
  - **Separator** – Define a separator if multiple values are specified.
  - **CaseSensitive** – Define if the attribute being tested for must match the case exactly.
  - **Value** – Define one or more values for the test, use the separator specified before to separate the values.

FileProperty

This test type will be represented by the Element <FileProperty>. For example:

```
- <FileProperty ValidWhen="true">
    <ListLoc Status="Fail" Type="Invalid"/>
      <!-- Support kb(KB), mb(MB), gb(GB)-->
    <Size MaxValue="20kb"/>
  - <Type>
      <TextCompare Separator="," CompareType="MustContain"
        CaseSensitive="No">text/html,image/gif,image/jpeg,text/xhtml,text/xml,text/css</TextCompare>
    </Type>
      <!-- For links inside the page-->
  - <Filter>
      <TextCompare Separator="," CompareType="MustNotContain" CaseSensitive="No">not test</TextCompare>
      <TextCompare Separator="," CompareType="MustNotContain" CaseSensitive="No">/bin/,.exe</TextCompare>
    </Filter>
  </FileProperty>
```

Figure 33: FileProperty check.

FileProperty

The **FileProperty** section contains the following attributes:

- **ValidWhen** – This is used to indicate if the result is valid when the condition is one of two values: **True** or **False**

ListLoc

The **ListLoc** section contains the following attributes:

- **Type** – There are two values for this attribute, **Valid** and **Invalid**. All elements that are considered valid or invalid are stored to the database (the Location).
- **Status** – This is used to indicate the disposition of the element and the severity selected by the user.

Size

The **Size** section contains the following attribute:

- **MaxValue** – Specify a value as the maximum size.

Type

The **Type** section contains the following attributes:

- **CompareType** – Define a compare type. The attributes for **CompareType** are **MustContain** and **MustEqual**.
- **Separator** – Define a separator if multiple values are specified.
- **CaseSensitive** – Define if the element being tested for must match the case exactly.
- **Value** – Define one or more Content-types for the test, use the separator specified before to separate the values.

Filter

This element is optional. The **Filter** section contains the following attributes:

- **CompareType** – Define a compare type. The attributes for **CompareType** are **MustNotContain** and **MustNotEqual**.
- **Separator** – Define a separator if multiple values are specified.
- **CaseSensitive** – Define if the element being tested for must match the case exactly.
- **Value** – Define one or more values for the test, use the separator specified before to separate the values.

LinkValidation

This test type will be represented by the Element <LinkValidation>. For example:

```
- <LinkValidation ValidWhen="true" ValidateFrames="True" TrueIf="All" ResultNA="NAResult" ValidateBookmarks="True"
  GetAllowCallHead="False">
      <ListLoc Status="Fail" Type="Invalid"/>
      <LinkSuccessStatusCode Separator=",">200</LinkSuccessStatusCode>
    - <Filter>
          <TextCompare Separator="," CompareType="MustNotContain" CaseSensitive="No">not test</TextCompare>
          <TextCompare Separator="," CompareType="MustNotContain" CaseSensitive="No">/bin/,.exe</TextCompare>
      </Filter>
    - <Attributes>
          <Attribute Attribute="href" Node="a"/>
          <Attribute Attribute="src" Node="img"/>
          <Attribute Attribute="src" Node="script"/>
          <Attribute Attribute="src" Node="embed"/>
          <Attribute Attribute="action" Node="form"/>
          <Attribute Attribute="href" Node="link"/>
          <Attribute Attribute="data" Node="object"/>
          <Attribute Attribute="src" Node="source"/>
          <Attribute Attribute="src" Node="track"/>
          <Attribute Attribute="src" Node="video"/>
          <Attribute Attribute="src" Node="audio"/>
          <Attribute Attribute="src" Node="input"/>
      </Attributes>
  </LinkValidation>
```

Figure 34: LinkValidation check.

LinkValidation

The **LinkValidation** section contains the following attributes:

- **ValidWhen** – This is used to indicate if the result is valid when the condition is one of two values: **True** or **False**.
- **TrueIf** – There are two values for this attribute: **All** and **One**. If **One** is defined, the scan will stop when one instance is found (to save scan time). If **All** is defined, the scan will only stop when all instances are found.
- **ResultNA** – Define a result when no link is found. If **TrueResult** is selected, then if no link is found, the True result will be returned. If **FalseResult** is defined, then if no link is found, the False result will be returned. If **NAResult** is defined, then if no link is found, the status of the tested file will be **Not Applicable**, which will be displayed in the Compliance Guardian Online report. In other words, you have the option to set the result to **Not Applicable** if none of the links are found.
- **ValidateBookmarks** – Define **True** or **False** for this attribute. If **True** is defined, the check will check whether the bookmarks work. If **False** is defined, the check will not check the bookmarks.
- **GetAllowCallHead** – Define **True** or **False** for this attribute. If **True** is defined, the link will be checked using the HEAD method, if the corresponding server does not support the HEAD method, the GET method will be used. If **False** is defined, the link will be checked using the HEAD method, if the corresponding server does not support the HEAD method, the GET method will not be used.

ListLoc

The **ListLoc** section contains the following attributes:

- **Type** – There are two values for this attribute, **Valid** and **Invalid**. All elements that are considered valid or invalid are stored to the database (the Location).
- **Status** – This is used to indicate the disposition of the element and the severity selected by the user.

Filter

The **Filter** section contains the following attributes:

- **CompareType** – Define a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustMatch**, **MustNotMatch**, **MustEqual**, and **MustNotEqual**.
- **Separator** – Define a separator if multiple values are specified.
- **CaseSensitive** – Define if the attribute name being tested for must match the case exactly.
- **Value** – Define one or more values for the test, use the separator specified before to separate the values.

Redaction

The Redaction check is used to redact the specified content in a file.

```
- <Redaction RedactMetadata="True" RedactType="Replace">
    - <FindText CompareType="MustEqual" CaseSensitive="No" ListLocStatus="Fail" SearchAll="Yes"
      ListLoc="Yes">
        - <Dictionary Separator=",">
            <![CDATA[{disallowed word list}]]>
          </Dictionary>
      </FindText>
      <Replace Repeat="True" AfterCount="0" BeforeCount="0" Type="Word">***</Replace>
  </Redaction>
```

Figure 35: Redaction type check.

Configuring Attributes for Redaction Type Check

Configure the attributes for the Redaction type check according to the instructions in the following sections.

Redaction

Configure the following attributes under this element:

- **RedactMetadata –** Select **True** or **False** for the attribute. You can select **True** to scan metadata.

- **RedactType** – Select a value for this attribute: **Delete** or **Replace**. If **Delete** is specified, the found instance will be deleted directly during the scan; if **Replace** is specified, you must specify a value and configure the related attributes, refer to Replace. The found instance will be replaced with the value you specified.

FindText

This element has the following attributes:

- **SearchAll** – Define whether or not to check the comments and scripts.
- **ListLoc** – Define whether or not to record the instance's location in the Compliance Guardian Online database. If **Yes** is specified, every location of the instance found will be recorded in the Compliance Guardian Online database. If **No** is specified, the check continues, but the locations of the instances found will not be recorded in the database.
- **ListLocStatus** – Define the status for the instance that is found. The status will be recorded in the Compliance Guardian Online database.

  ***Note:** If the status set for **True result** or **False result** is **Fail**, the value for the **Status** attribute will be **Fail**, and the value cannot be changed.

- **CaseSensitive** – Define if the text being tested for must match the case exactly.
- **CompareType** – Define **MustContain** or **MustEqual** for this attribute.
- **Dictionary** – Configure the following attributes:
  - **Separator** – Define a separator if multiple values are specified.
  - **Value** – Define one or more values for the test, use the separator specified before to separate the values.

Regex

This element has the following attributes:

- **SearchAll** – Define whether or not to check the comments and scripts.
- **ListLoc** – Define whether or not to record the instance's location in the Compliance Guardian Online database. If **Yes** is specified, every location of the instance found will be recorded in the Compliance Guardian Online database. If **No** is specified, the check continues, but the locations of the instances found will not be recorded in the database.
- **ListLocStatus** – Define the status for the instance that is found. The status will be recorded in the Compliance Guardian Online database.

  ***Note:** If the status set for **True result** or **False result** is **Fail**, the value for the **Status** attribute will be **Fail**, and the value cannot be changed.

- **CaseSensitive** – Define if the text being tested for must match the case exactly.

- **Dictionary** – Configure the following attributes:
    - **Separator** – Define a separator if multiple values are specified.
    - **Value** – Define one or more values for the test, use the separator specified before to separate the values.
- **Filter** – This is optional. Select the checkbox before **Filter**, the **Text** section and the **Regex** section appear:
    - **Text** – Configure the following attributes:
        - **CaseSensitive** – Define if the element being tested for must match the case exactly.
        - **Separator** – Specify a separator if multiple values are specified.
        - **Value** – Define one or more values for the test, and use the separator specified before to separate the values. If the scanned result that matches the specified regular expression exactly matches the value specified here, this result will be filtered out.
    - **Regex** – Configure the following attributes:
        - **CaseSensitive** – Define if the element being tested for must match the case exactly.
        - **Value** – Define a regular expression. If the scanned result that matches the specified regular expression also matches the regular expression specified here, this result will be filtered out.

Replace

If **Replace** is selected as the value of the **RedactType** attribute, you must configure this node. Configure the following attributes:

- **Type** – Select to redact a word or a section.
- **BeforeCount** – If you specify **Section** for the **Type** attribute, you must configure this attribute. Specify the number of the characters before the value you specified. The characters in the range of the specified number will also be redacted.
- **AfterCount** – If you specify **Section** for the **Type** attribute, you must configure this attribute. Specify the number of the characters after the value you specified. The characters in the range of the specified number will also be redacted.
- **Repeat** – Define whether or not to repeat the specified value to make sure the replaced result keeping the same length as the original value.
- **Value** – Define the value that is used to replace the found instance.

Test Suites

A test suite is a logical grouping of test definition files, or a set of checks, that define how to present the scanned data. Test suites allow you to build scan plans for your specific regulations and requirements. These collections are the basis of Compliance Guardian Online scans. A test suite contains one or more checks and a configuration file that is used to define how to combine these checks and set risk levels for scan results.

Test Suite for Compliance Reporting

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright 2001-2014 AvePoint All Rights Reserved. -->
- <CCC Version="3.3.0.0000" IsAccessibility="true">
    <Name>Section 508</Name>
    <Description>US Section 508</Description>
  - <TDFs>
    - <RunAsTestGroup DatabaseField="TDFResult5" MainTdfID="508_html_A_qaqa">
        <Name>Section 508 1194.22 (a)</Name>
        <PolicyURL>http://www.access-board.gov/sec508/guide/1194.22.htm#(a)</PolicyURL>
        <Description>(a) A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content). This Check can be customized.</Description>
        <DoRunTDF RiskLevel="3" RunCheck="True" tdfID="508_html_1_qaqa"/>
        <DoRunTDF RiskLevel="3" RunCheck="True" tdfID="508_html_2_qaqa"/>
        <DoRunTDF RiskLevel="3" RunCheck="True" tdfID="508_html_3_qaqa"/>
      </RunAsTestGroup>
    - <RunAsTestGroup DatabaseField="TDFResult6" MainTdfID="508_html_B_qaqa">
        <Name>Section 508 1194.22 (b)</Name>
        <PolicyURL>http://www.access-board.gov/sec508/guide/1194.22.htm#(b)</PolicyURL>
        <Description>Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation. This Check can be customized.</Description>
        <DoRunTDF RiskLevel="3" RunCheck="True" tdfID="508_html_4_qaqa"/>
        <DoRunTDF RiskLevel="3" RunCheck="True" tdfID="508_html_5_qaqa"/>
        <DoRunTDF RiskLevel="3" RunCheck="True" tdfID="508_html_6_qaqa"/>
      </RunAsTestGroup>
      <DoRunTDF DatabaseField="TDFResult21" RiskLevel="3" RunCheck="True" tdfID="508_html_8C"/>
    - <RunAsTestGroup DatabaseField="TDFResult7" MainTdfID="508_html_D_qaqa">
        <Name>Section 508 1194.22 (d)</Name>
        <PolicyURL>http://www.access-board.gov/sec508/guide/1194.22.htm#(d)</PolicyURL>
        <Description>Documents shall be organized so they are readable without requiring an associated style sheet. This Check can be customized.</Description>
        <DoRunTDF RiskLevel="3" RunCheck="True" tdfID="508_html_8_qaqa"/>
        <DoRunTDF RiskLevel="3" RunCheck="True" tdfID="508_html_9_qaqa"/>
      </RunAsTestGroup>
      <DoRunTDF DatabaseField="TDFResult8" RiskLevel="3" RunCheck="True" tdfID="508_html_10_qaqa"/>
      <DoRunTDF DatabaseField="TDFResult9" RiskLevel="3" RunCheck="True" tdfID="508_html_11_qaqa"/>
    - <RunAsTestGroup DatabaseField="TDFResult3" MainTdfID="508_html_GH_qaqa">
        <Name>Section 508 1194.22 (g)(h)</Name>
        <PolicyURL>http://www.access-board.gov/sec508/guide/1194.22.htm#(g)</PolicyURL>
        <Description>(g) Row and column headers shall be identified for data tables. (h) Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.</Description>
        <DoRunTDF RiskLevel="3" RunCheck="True" tdfID="508_html_12_qaqa"/>
        <DoRunTDF RiskLevel="3" RunCheck="True" tdfID="508_html_13_qaqa"/>
      </RunAsTestGroup>
      <DoRunTDF DatabaseField="TDFResult2" RiskLevel="3" RunCheck="True" tdfID="508_html_14_qaqa" Role="MaxRow"/>
      <DoRunTDF DatabaseField="TDFResult4" RiskLevel="3" RunCheck="True" tdfID="508_html_15_qaqa" Role="DataTable"/>
    - <RunAsTestGroup DatabaseField="TDFResult10" MainTdfID="508_html_I_qaqa">
        <Name>Section 508 1194.22 (i)</Name>
        <PolicyURL>http://www.access-board.gov/sec508/guide/1194.22.htm#(i)</PolicyURL>
        <Description>Frames shall be titled with text that facilitates frame identification and navigation.</Description>
        <DoRunTDF RiskLevel="3" RunCheck="True" tdfID="508_html_16_qaqa"/>
        <DoRunTDF RiskLevel="3" RunCheck="True" tdfID="508_html_17_qaqa"/>
        <DoRunTDF RiskLevel="3" RunCheck="True" tdfID="508_html_29_qaqa"/>
      </RunAsTestGroup>
    - <RunAsTestGroup DatabaseField="TDFResult11" MainTdfID="508_html_J_qaqa">
        <Name>Section 508 1194.22 (j)</Name>
        <PolicyURL>http://www.access-board.gov/sec508/guide/1194.22.htm#(j)</PolicyURL>
        <Description>Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz. This check can be customized.</Description>
        <DoRunTDF RiskLevel="3" RunCheck="True" tdfID="508_html_18_qaqa"/>
        <DoRunTDF RiskLevel="3" RunCheck="True" tdfID="508_html_19_qaqa"/>
      </RunAsTestGroup>
      <DoRunTDF DatabaseField="TDFResult16" RiskLevel="3" RunCheck="True" tdfID="508_html_20_qaqa"/>
      <DoRunTDF DatabaseField="TDFResult12" RiskLevel="3" RunCheck="True" tdfID="508_html_21_qaqa"/>
      <DoRunTDF DatabaseField="TDFResult22" RiskLevel="3" RunCheck="True" tdfID="508_html_m"/>
      <DoRunTDF DatabaseField="TDFResult13" RiskLevel="3" RunCheck="True" tdfID="508_html_22_qaqa"/>
      <DoRunTDF DatabaseField="TDFResult14" RiskLevel="3" RunCheck="True" tdfID="508_html_23_qaqa"/>
      <DoRunTDF DatabaseField="TDFResult15" RiskLevel="3" RunCheck="True" tdfID="508_html_24_qaqa"/>
    </TDFs>
</CCC>
```

Figure 36: Overview of the test suite.

The following basic attributes are in the test suite:

- **IsAccessibility** – Select whether or not to check the file accessibility. If **true** is selected, the file will be scanned keeping its formatting. If **false** is selected, the file will be

scanned, stripping out its formatting. If the file that will be scanned is the unsupported type in Compliance Guardian Online, the function will not be used no matter the **true** option or the **false** option is selected.

- **Version** – The version of the test suite.
- **DepthScan** – You can add this attribute to the root node **CCC**.
    - **Hybrid** – If you specify **Hybrid** as the value, Compliance Guardian Online scans the files with the supported file types. If the files that will be scanned are the unsupported types in Compliance Guardian Online, **IFilter** will be used for the scan. If you do not add the **DepthScan** in the test suite, **Hybrid** is the default option used for the scan.
    - **True** – If you specify **True** as the value, Compliance Guardian Online scans the files. If the files that will be scanned are the unsupported types in Compliance Guardian Online, the exception message will be thrown and displayed in Compliance Guardian Online Report.
    - **False** – If you specify **False** as the value, **IFilter** is used for the scan.

  For more information on the supported file types in Compliance Guardian Online, refer to Appendix D: Supported File Types in Compliance Guardian Online.

- **Name** – The identifying name of the file.
- **Description** – A brief description of the file.

RiskFormula

Risk Formula provides the user with a method to measure level of risk in proportion to the risk type. It allows users to grow risk at a specified factor, providing an accurate look at risk by occurrence.

You can add the **RiskFormulas** node that must be in parallel with the **Name** node in the test suite, and add the **Raw**, **Stepped**, and **Weighted** attributes, and then add the risk formulas as the values of the three attributes to define the Raw type risk formula, Stepped type risk formula and Weighted type risk formua.

RunAsTestGroup

A RunAsTestGroup groups the specified checks together. The checks can test files according to one checkpoint.

- **DatabaseField** – This is the location in the Compliance Guardian Online database where the scan result data is stored. Compliance Guardian Online will automatically specify the location for storing data.
- **MaintdfID** – Provides the ID of the check to be run and stored in the database table.
- **Name** – Provides the name of the checkpoint.

- **PolicyURL** – Define a URL that will link to a website defining rules for how checks in this check group will test files.
- **Description** – Enter the description for the test group. In Scan Result of Compliance Reports, the description will display in the file's corresponding detailed report.
- **ContentType** – You can add this attribute in the **Operator** node in **Compliance Guardian Online** > **Test Suite Manager** > **Edit Test Suite Attributes** interface. Define the content types that will be scanned. If you do not define the content types, all the file content types that are supported to be scanned in Compliance Guardian Online.
- **Operator** – If you add the **AND** or **OR** node, you cannot add other **DoRunTDF** nodes under this **RunAsTestGroup**, you can only add **DoRunTDF** nodes under the **AND** or **OR** node. Configure the following attributes:
    - **True** – Specify the result of the check group according to the check result. The result of the check group will be the value defined here if the check result is True.
    - **False** – Specify the result of the check group according to the check result. The result of the check group will be the value defined here if the check result is False.
    - **NA** – Specify the result of the check group according to the check result. The result of the check group will be the value defined here if the check result is NA.
    - **DoRunTDF** – Configure the following attributes:
        - **tdfID** – Provide the ID of the check to be run and stored in the database table.
        - **RunCheck** – If **True** is defined for this attribute, when running a Compliance Guardian Online job using the test suite, the files will be scanned according to the rule set in this check. If **False** is defined for this attribute, the corresponding check will not be used to scan the files.
        - **RiskLevel** – Specify the risk level for this check. RiskLevel(r1) is required, RiskLevel(r2) and RiskLevel(r3) are optional. Use comma (**,**) to separate them.
            - **RiskLevel(r1)** – The Item Initial Risk value assigned on the initial occurrence of the compliance failure (related to the check being tested for) in the document or stream. Allowed values for **RiskLevel(r1)** are 1 to 10.
            - **RiskLevel(r2)** – The Item Additional Risk Level factor that the risk level grows at for every additional failure at the check level (for the same type) found in the document or stream. This number is optional where the integer "-1" means ignore the value (allowing to use the third value). If the value is -1 then the factor will be 1. Allowed values are -1 and 1 to 10.

- **RiskLevel(r3) –** The Item risk in relation to other checks. This Item is optional. If this number is missing then it is assumed that its value is “1”. Allowed values are 1-10.

- **TrueIf** – Select which check results will be considered True in this check group. For example: if you just specify a check, and then select **Pass** and **HR** for the **TrueIf** attribute. When the result of the check is **Pass** or **HR**, the check result in this check group is considered True.
  - When all of the checks’ results in this check group are True, the result of this check group is considered True.
  - If you have added **AND**:

    When you add multiple checks, one of the checks’ results in this test suite is **False**, and the check with a **False** check result is not the last check specified under the Operator node, the result of the checks is **NA**. If the check with a **False** check result is the last check you added in the Operator node, then the result of the checks added is **False**.
  - If you have added **Or**:

    When you add multiple checks, one of the checks’ results in this test suite is **True**, and the check with a **True** check result is not the last check you added in the Operator node, the result of the checks added in the Operator node is **NA**. If the check with a **True** check result is the last check you added in the Operator node, the result of the checks added in the Operator node is **True**.

- **ContentType** – You can add this attribute in the **Operator** node in **Compliance Guardian Online** > **Test Suite Manager** > **Edit Test Suite Attributes** interface. Define the content types that will be scanned. If you do not define the content types, all the file content types that are supported to be scanned in Compliance Guardian Online will be scanned.

DoRunCheck

A DoRunCheck keeps specified checks separately. They will not run as a group, but will scan files separately.

- **DatabaseField** – This is the location in the Compliance Guardian Online database where the scan result data is stored. Compliance Guardian Online will automatically specify the location for storing data.
- **RiskLevel** – Specify the risk level for this check. RiskLevel(r1) is required, RiskLevel(r2) and RiskLevel(r3) are optional. Use comma (**,**) to separate them.

- **RiskLevel(r1)** – The Item Initial Risk value assigned on the initial occurrence of the compliance failure (related to the check being tested for) in the document or stream. Allowed values for **RiskLevel(r1)** are 1 to 10.
- **RiskLevel(r2)** – The Item Additional Risk Level factor that the risk level grows at for every additional failure at the check level (for the same type) found in the document or stream. This number is optional where the integer "-1" means ignore the value (allowing to use the third value). If the value is -1 then the factor will be 1. Allowed values are -1 and 1 to 10.
- **RiskLevel(r3)** – The Item risk in relation to other checks. This Item is optional. If this number is missing then it is assumed that its value is "1". Allowed values are 1-10.

- **ContentType** – You can add this attribute in the node in **Compliance Guardian Online** > **Test Suite Manager** > **Edit Test Suite Attributes** interface. Define the content types that will be scanned. If you do not define the content types, all the file content types that are supported to be scanned in Compliance Guardian Online will be scanned.
- **Role** – You can add this attribute in the node in **Compliance Guardian Online** > **Test Suite Manager** > **Edit Test Suite Attributes** interface. Assign a role to the corresponding check.
  - **MaxRow** – After scanned by the check that is assigned to the **MaxRow** role, the failed files will be reported in the Compliance File Errors Report, the error type of the failed file is Maximum Row Exception.
  - **DataTable** – After scanned by the check that is assigned to the **DataTable** role, the locations of the instances that are recorded will be reported in the Compliance Data Table Report.
  - **Cookie** – The check that is assigned this role can be used for the Cookie check.
- **RunCheck** – If **True** is selected for this attribute, when running a Compliance Guardian Online job using the test suite, the files will be scanned according to the rule set in this check. If **False** is selected for this attribute, the check will not be used to scan the files.
- **TdfID** – Provide the ID of the check to be run and stored in the database table.

Test Suite for Classification and Tagging

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright 2001-2014 AvePoint All Rights Reserved. -->
- <Classification Version="3.3.0.0002" DepthScan="HyBrid">
    <Name>classification</Name>
    <Description/>
  - <TagName NoRisk="False" overrideuser="false" OverrideCG="True" placetags="1" tag="category">
    - <RiskFormulas>
        <Raw Name="Raw">r1*n</Raw>
        <Stepped Name="Stepped">r1+r2*(n-1)</Stepped>
        <Weighted Name="Weighted">r1+r2*r3*(n-1)</Weighted>
      </RiskFormulas>
    - <AllowedTagValues>
        <TagValue DefaultRiskValue_Weighted="3" DefaultRiskValue_Stepped="2" DefaultRiskValue_Raw="1"
          priority="1">fruit</TagValue>
        <TagValue DefaultRiskValue_Weighted="0" DefaultRiskValue_Stepped="0" DefaultRiskValue_Raw="0"
          priority="2">vagetable</TagValue>
        <TagValue DefaultRiskValue_Weighted="0" DefaultRiskValue_Stepped="0" DefaultRiskValue_Raw="0"
          priority="3">fish</TagValue>
      </AllowedTagValues>
    - <automated>
      - <tdfidgroup>
          <tdfid refine="True" NA="fish" False="vagetable" True="fruit" id="67ed6aad-66f4-4203-8241-27221e979889"
            RiskLevel="1,1,1"/>
        </tdfidgroup>
      </automated>
    </TagName>
  - <TagName NoRisk="False" overrideuser="false" OverrideCG="True" placetags="3" tag="dailylife">
    - <RiskFormulas>
        <Raw Name="Raw">r1*n</Raw>
        <Stepped Name="Stepped">r1+r2*(n-1)</Stepped>
        <Weighted Name="Weighted">r1+r2*r3*(n-1)</Weighted>
      </RiskFormulas>
    - <AllowedTagValues>
        <TagValue DefaultRiskValue_Weighted="3" DefaultRiskValue_Stepped="2" DefaultRiskValue_Raw="1"
          priority="1">sockets</TagValue>
        <TagValue DefaultRiskValue_Weighted="0" DefaultRiskValue_Stepped="0" DefaultRiskValue_Raw="0"
          priority="2">hat</TagValue>
        <TagValue DefaultRiskValue_Weighted="0" DefaultRiskValue_Stepped="0" DefaultRiskValue_Raw="0"
          priority="3">shoes</TagValue>
      </AllowedTagValues>
    - <automated>
      - <tdfidgroup>
          <tdfid refine="True" NA="shoes" False="hat" True="sockets" id="67ed6aad-66f4-4203-8241-27221e979889"
            RiskLevel="1,1,1"/>
        </tdfidgroup>
      </automated>
    </TagName>
</Classification>
```

Figure 37: Overview of the test suite.

The following basic attributes are in the test suite:

- **Version** – The version of the test suite.
- **Name** – The identifying name of the file.
- **Description** – A brief description of the file.

TagName

Configure the following attributes in the **TagName** node:

- **Tag** – Specify the name of the metadata element that will be created.
- **PlaceTags** – Define where the tag will be placed. There are four values for this attribute:

- **0** – Do not add tag to the file and SharePoint
- **1** – Add the tag to the file only
- **2** – Add the tag to the file and SharePoint
- **3** – Add the tag to SharePoint only

- **OverrideUser** – If the specified metadata already exists, select whether or not to override the original metadata.
- **OverrideCG** – If the value of **OverrideUser** is **Yes**, the **OverrideCG** attribute will not take effect. If the value of **OverrideUser** is **No**, the **OverrideCG** attribute will take effect.

  If the value of **OverrideCG** is **True**, the tag value of this scan will be used to do the corresponding Classification action.

  If the value of **OverrideCG** is **False**, the original file's tag value will be used to do the corresponding Classification action. In this case, there are the following conditions:

  - If there is one original tag value in the file or in SharePoint, the value is used to do the Classification action.
  - If there are two original values (one is in file, one is in SharePoint), the one that will be used to do the action depends on the priority we specified for the **AllowedTagValues** attribute in this test suite.
    - If the two original values are also specified for the **AllowedTagValues** attribute of this test suite, the one that will be used to do the action depends on the priority we specified for the **AllowedTagValues** attribute of this test suite.
    - If one of the two original values is specified for the **AllowedTagValues** attribute of this test suite, Compliance Guardian Online will compare the priority of the original tag value and the tag value in this scan. The one with the higher priority will be used to do the corresponding Classification action.
    - If none of the two original values is specified in this test suite, the tag value of this scan will be used to do the corresponding Classification action.
- **NoRisk** – If you select **False** as the value of the **NoRisk** attribute, you must add the **RiskFormula** node in the test suite. You are not required to define the risk formulas if you set the value to **True**.

  If you have selected **False** as the value of the **NoRisk** attribute, you must add the **RiskFormula** node under the **TagName** node. Then, add the **Raw**, **Stepped**, and **Weighted** attributes in the node, and add the risk formulas as the values of the three attributes to define the Raw type risk formula, Stepped type risk formula and Weighted type risk formua.

AllowedTagValues

Configure the following attributes for this element:

- **DefaultRiskValue_Raw** – Enter a value as the raw risk score of the file. The attribute will take effect when the value of **OverrideUser** is **No**. When the original file's metadata is not overridden, the risk score is not calculated by the Raw type risk formula that is selected in the **RiskFormula** element field of the test suite. The risk core is the value you specified here.
- **DefaultRiskValue_Stepped** – Enter a value as the stepped risk score of the file. The attribute will take effect when the value of **OverrideUser** is **No**. When the original file's metadata is not overridden, the risk score is not calculated by the Stepped type risk formula that is selected in the **RiskFormula** element field of the test suite. The risk core is the value you specified here.
- **DefaultRiskValue_Weighted** – Enter a value as the weighted risk score of the file. The attribute will take effect when the value of **OverrideUser** is **No**. When the original file's metadata is not overridden, the risk score is not calculated by the Weighted type risk formula that is selected in the **RiskFormula** element field of the test suite. The risk core is the value you specified here.
- **Priority** – Specify the priority of the tag value. When scanning a file, different checks will return different scan results. This is used to determine which tag value will be added to the file.
- **Value** – Specify the tag value. If you do not want to add a tag value to a scanned file, leave this value empty.

CheckIdGroup

Configure the following attributes for this element:

- **id** – Provide the ID of the check to be run and stored in the database table.
- **True** – Select a value. If the test of this check evaluates to True, then the tag value will be this one.
- **False** – Select a value. If the test of this check evaluates to False, then the tag value will be this one.
- **N/A** – Select a value. If the test of this check evaluates to N/A, then the tag value will be this one.
- **RiskLevel** – Specify the risk level for this check. RiskLevel(r1) is required, RiskLevel(r2) and RiskLevel(r3) are optional. Use comma (**,**) to separate them.
    - **RiskLevel(r1)** – The Item Initial Risk value assigned on the initial occurrence of the compliance failure (related to the check being tested for) in the document or stream. Allowed values for **RiskLevel(r1)** are 1 to 10.
    - **RiskLevel(r2)** – The Item Additional Risk Level factor that the risk level grows at for every additional failure at the check level (for the same type) found in the

document or stream. This number is optional where the integer "-1" means ignore the value (allowing to use the third value). If the value is -1 then the factor will be 1. Allowed values are -1 and 1 to 10.

- **RiskLevel(r3)** – The Item risk in relation to other checks. This Item is optional. If this number is missing then it is assumed that its value is "1". Allowed values are 1-10.

- **Refine** – If you set **False** as the value, the following checks specified in the group will not be taken effect. If you set **True** as the value, all of the specified checks will be used for the scan.

Operator

Add the **AND** or **OR** node, and configure the following attributes:

- **True** – Specify the result of the check group according to the check result. The result of the check group will be the value defined here if the check result is True.
- **False** – Specify the result of the check group according to the check result. The result of the check group will be the value defined here if the check result is False.
- **NA** – Specify the result of the check group according to the check result. The result of the check group will be the value defined here if the check result is NA.
- **Refine –** Define if the next **AND** or **Or** node will be used to scan files.
- **tdfID** – Provide the ID of the check to be run and stored in the database table.
  - **RunCheck** – If **True** is defined for this attribute, when running a Compliance Guardian Online job using the test suite, the files will be scanned according to the rule set in this check. If **False** is defined for this attribute, the corresponding check will not be used to scan the files.
- **RiskLevel** – Specify the risk level for this check. RiskLevel(r1) is required, RiskLevel(r2) and RiskLevel(r3) are optional. Use comma (**,**) to separate them.
  - **RiskLevel(r1)** – The Item Initial Risk value assigned on the initial occurrence of the compliance failure (related to the check being tested for) in the document or stream. Allowed values for **RiskLevel(r1)** are 1 to 10.
  - **RiskLevel(r2)** – The Item Additional Risk Level factor that the risk level grows at for every additional failure at the check level (for the same type) found in the document or stream. This number is optional where the integer "-1" means ignore the value (allowing to use the third value). If the value is -1 then the factor will be 1. Allowed values are -1 and 1 to 10.
  - **RiskLevel(r3)** – The Item risk in relation to other checks. This Item is optional. If this number is missing then it is assumed that its value is "1". Allowed values are 1-10.
- **TrueIf** – Select which check results will be considered True in this check group. For example: if you just select a check, and then select **Pass** and **HR** for the **TrueIf** attribute.

When the result of the check is **Pass** or **HR**, the check result in this check group is considered True.

- When all of the checks' results in this check group are True, the result of this check group is considered True.
- If you have added **AND**:

  When you add multiple checks, one of the checks' results in this test suite is **False**, and the check with a **False** check result is not the last check specified under the Operator node, the result of the checks is **NA**. If the check with a **False** check result is the last check you added in the Operator node, then the result of the checks added is **False**.

- If you have added **Or**:

  When you add multiple checks, one of the checks' results in this test suite is **True**, and the check with a **True** check result is not the last check you added in the Operator node, the result of the checks added in the Operator node is **NA**. If the check with a **True** check result is the last check you added in the Operator node, the result of the checks added in the Operator node is **True**.

Test Suite for Redaction

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright 2001-2014 AvePoint All Rights Reserved. -->
- <Classification Version="3.3.0.0000" Redaction="True">
    <Name>Redact Disallowed Words with Asterisk</Name>
    <Description>Compliance Guardian will redact disallowed words with *** in the document. (This is
      an example Test Suite for Compliance Guardian Redaction Action. You need to modify the
      Checks in the Test Suite for listing disallowed words based on your rule.)</Description>
  - <Action RedactOfficeMetadata="True" NoRisk="True" Type="Redaction">
      - <tdfidgroup>
          <tdfid RiskLevel="1,1,1" id="4760e1ae-ba16-4031-93cd-98bf4add23ba"/>
        </tdfidgroup>
    </Action>
</Classification>
```

Figure 38: Overview of the test suite.

The following basic attributes are in the test suite:

- **Version** – The version of the test suite.
- **Name** – The identifying name of the file.
- **Description** – A brief description of the file.

Action

- **NoRisk** – If you select **False** as the value of the **NoRisk** attribute, you must add the **RiskFormula** node in the test suite. You are not required to define the risk formulas if you set the value to **True**.

If you have selected **False** as the value of the **NoRisk** attribute, you must add the **RiskFormula** node under the **Action** node. Then, add the **Raw**, **Stepped**, and **Weighted** attributes in the node, and add the risk formulas as the values of the three attributes to define the Raw type risk formula, Stepped type risk formula and Weighted type risk formula.

- **RedactOfficeMetadata** – Specify whether to redact the office metadata.

checkIdgroup

Configure the following attributes:

- **id** – Specify the ID of a Redaction type check.
- **RiskLevel** – Specify the risk level for this check. RiskLevel(r1) is required, RiskLevel(r2) and RiskLevel(r3) are optional. Use comma (**,**) to separate them.
    - **RiskLevel(r1)** – The Item Initial Risk value assigned on the initial occurrence of the compliance failure (related to the check being tested for) in the document or stream. Allowed values for **RiskLevel(r1)** are 1 to 10.
    - **RiskLevel(r2)** – The Item Additional Risk Level factor that the risk level grows at for every additional failure at the check level (for the same type) found in the document or stream. This number is optional where the integer "-1" means ignore the value (allowing to use the third value). If the value is -1 then the factor will be 1. Allowed values are -1 and 1 to 10.
    - **RiskLevel(r3)** – The Item risk in relation to other checks. This Item is optional. If this number is missing then it is assumed that its value is "1". Allowed values are 1-10.

Appendix D: Supported File Types

Condition	File Type
Supported for Scanning	DOC
	DOCX
	XLS
	XLSX
	PPT
	PPTX
	PDF
	ASP
	ASPX
	HTM
	HTML
	TXT
	XML
	ZIP
	JSP
	PHP
	DOCM
	DOTX
	DOTM
	XLSM
	XLTM
	XLAM
	XLTX
	XLSB
	XLT
	XLA
	PPTM
	POTX
	POTM
	PPSX
	PPSM
	POT
	PPS

***Note:** PDFs with unstructured textual content are not supported to be scanned in Compliance Guardian Online.

Notices and Copyright Information

Notice
The materials contained in this publication are owned or provided by AvePoint, Inc. and are the property of AvePoint or its licensors, and are protected by copyright, trademark and other intellectual property laws. No trademark or copyright notice in this publication may be removed or altered in any way.

Copyright
Copyright © 2013-2015 AvePoint, Inc. All rights reserved. All materials contained in this publication are protected by United States and international copyright laws and no part of this publication may be reproduced, modified, displayed, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of AvePoint, 3 Second Street, Jersey City, NJ 07311, USA or, in the case of materials in this publication owned by third parties, without such third party's consent. Notwithstanding the foregoing, to the extent any AvePoint material in this publication is reproduced or modified in any way (including derivative works and transformative works), by you or on your behalf, then such reproduced or modified materials shall be automatically assigned to AvePoint without any further act and you agree on behalf of yourself and your successors, assigns, heirs, beneficiaries, and executors, to promptly do all things and sign all documents to confirm the transfer of such reproduced or modified materials to AvePoint.

Trademarks
AvePoint®, DocAve®, the AvePoint logo, and the AvePoint Pyramid logo are registered trademarks of AvePoint, Inc. with the United States Patent and Trademark Office. These registered trademarks, along with all other trademarks of AvePoint used in this publication are the exclusive property of AvePoint and may not be used without prior written consent.

Microsoft, MS-DOS, Internet Explorer, Office, Office 365, SharePoint, Windows PowerShell, SQL Server, Outlook, Windows Server, Active Directory, and Dynamics CRM 2013 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe Acrobat and Acrobat Reader are trademarks of Adobe Systems, Inc.

All other trademarks contained in this publication are the property of their respective owners and may not be used without such party's consent.

Changes
The material in this publication is for information purposes only and is subject to change without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, AvePoint makes no representation or warranty, expressed or implied, as to its completeness, accuracy, or suitability, and assumes no liability resulting from errors or omissions in this publication or from the use of the information contained herein. AvePoint reserves the right to make changes in the Graphical User Interface of the AvePoint software without reservation and without notification to its users.

AvePoint, Inc.
Harborside Financial Center, Plaza 10
3 Second Street, 9th Floor
Jersey City, New Jersey 07311